高等院校计算机实验与实践系列示范教材

网络与信息安全实验教程

赵华伟 刘理争 编著

清华大学出版社

高等院校计算机实验与实践系列示范教材

网络与信息安全实验教程

赵华伟　刘理争　编著

清华大学出版社
北　京

内 容 简 介

本教程是作者依据多年在网络信息安全领域的教学、培训和技术实践，针对高等院校网络信息安全及相关本科和研究生专业的教学特点和需求，以及高校实验室的建设现状，从实用性的角度出发编写而成。

全书共分3篇。第1篇(实验1～实验3)为基础篇，着重介绍实验环境的搭建、常用的系统命令以及系统的安全配置方法；第2篇(实验4～实验13)为安全操作篇，着重讲解NTFS的使用方法、账号的保护、文件的加密、电子邮件的加密与签名、IIS安全配置以及SSL配置实验等；第3篇(实验14～实验18)为攻击体会篇，着重讲解了对Windows系统账号的攻击方法、ARP攻击方法、远程控制攻击、映像劫持攻击以及SQL注入攻击等。本教程的所有实验均基于VMware虚拟机平台的TEAM功能搭建，使学生在一台计算机上就能独立完成基于局域网的实验项目，从而能有效帮助学生巩固网络信息安全课程的基础理论知识，更深入地掌握网络信息安全的各项操作技能。

本书不仅适用于高等院校的信息安全专业、计算机专业的高年级本科生、研究生作为实验教材使用，也适用于作为网络信息安全职业技术培训实验教材，同时也可作为对网络信息安全技术有兴趣的读者的参考用书。

图书在版编目(CIP)数据

网络与信息安全实验教程/赵华伟，刘理争编著.--北京：清华大学出版社，2012.1
(高等院校计算机实验与实践系列示范教材)
ISBN 978-7-302-26823-9

Ⅰ.①网… Ⅱ.①赵…②刘… Ⅲ.①计算机网络－安全技术－高等学校－教材
Ⅳ.①TP393.08

中国版本图书馆CIP数据核字(2011)第186921号

责任编辑：索 梅
责任校对：白 蕾
责任印制：

出版发行：清华大学出版社 **地 址**：北京清华大学学研大厦A座
http://www.tup.com.cn **邮 编**：100084
社 总 机：010-62770175 **邮 购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经 销：全国新华书店
开 本：185×260 **印 张**：13 **字 数**：325千字
版 次：2012年1月第1版 **印 次**：2012年1月第1次印刷
印 数：1～ 000
定 价： .00元

产品编号：042629-01

出版说明

当前，重视实验与实践教育是各国高等教育界的发展潮流，我国与国外教学工作的差距也主要表现在实践教学环节上。面对新的形式和新的挑战，完善实验与实践教育体系成为一种必然。为了培养具有高质量、高素质、高实践能力和高创新能力的人才，全国很多高等院校在实验与实践教学方面进行了大力改革，在实验与实践教学内容、教学方法、教学体系、实验室建设等方面积累了大量的宝贵经验，起到了教学示范作用。

实验与实践性教学与理论教学是相辅相成的，具有同等重要的地位。它是在开放教育的基础上，为配合理论教学、培养学生分析问题和解决问题的能力以及加强训练学生专业实践能力而设置的教学环节；对于完成教学计划、落实教学大纲，确保教学质量，培养学生分析问题、解决问题的能力和实际操作技能更具有特别重要的意义。同时，实践教学也是培养应用型人才的重要途径，实践教学质量的好坏，实际上也决定了应用型人才培养质量的高低。因此，加强实践教学环节，提高实践教学质量，对培养高质量的应用型人才至关重要。

近年来，教育部把实验与实践教学作为对高等院校教学工作评估的关键性指标。2005 年 1 月，在教育部下发的《关于进一步加强高等学校本科教学工作的若干意见》中明确指出："高等学校要强化实践育人的意识，区别不同学科对实践教学的要求，合理制定实践教学方案，完善实践教学体系。要切实加强实验、实习、社会实践、毕业设计（论文）等实践教学环节，保障各环节的时间和效果，不得降低要求。"，"要不断改革实践教学内容，改进实践教学方法，通过政策引导，吸引高水平教师从事实践环节教学工作。要加强产学研合作教育，充分利用国内外资源，不断拓展校际之间、校企之间、高校与科研院所之间的合作，加强各种形式的实践教学基地和实验室建设。"

为了配合开展实践教学及适应教学改革的需要，我们在全国各高等院校精心挖掘和遴选了一批在计算机实验与实践教学方面具有潜心研究并取得了富有特色、值得推广的教学成果的作者，把他们多年积累的教学经验编写成教材，为开展实践教学的学校起一个抛砖引玉的示范作用。

为了保证出版质量，本套教材中的每本书都经过编委会委员的精心筛选和

严格评审，坚持宁缺毋滥的原则，力争把每本书都做成精品。同时，为了能够让更多、更好的实践教学成果应用于社会和各高等院校，我们热切期望在这方面有经验和成果的教师能够加入到本套丛书的编写队伍中，为实践教学的发展和取得成效做出贡献；也衷心地期望广大读者对本套教材提出宝贵意见，以便我们更好地为读者服务。

清华大学出版社

联系人：索梅 suom@tup.tsinghua.edu.cn

FOREWORD

前言

众所周知，网络技术和信息技术正以前所未有的速度发展和普及，给人们的生活和工作带来了巨大的便利，大幅提高了社会的运转效率。同时，我们应该看到，伴随着网络信息技术的发展，针对网络和信息安全的攻击非但没有得到有效遏制，反而愈演愈烈，严重干扰了人们的正常社会活动，成为影响社会稳定的不可忽视的因素。因此网络信息安全问题已成为当今信息社会必须面对和解决的重要问题。

解决网络信息安全问题的关键在于网络信息安全人才的培养。而目前在我国，能够熟练掌握网络信息安全技术，对信息系统进行合理安全配置的人才为数并不多，远远不能满足国家和各行业对网络信息安全人才日臻旺盛的需求。针对社会的这一需求，我们组织编写了本教材并完成了相关配套视频的制作，以期为培养出更多的具有实际操作能力的网络信息安全人才贡献一份力量。

1. 教程特色

本教材利用 VMware 虚拟机的 TEAM 功能，在 VMware 平台上搭建出一个包含不同 Windows 操作系统版本的局域网，使得实验操作者在一台计算机上即可完成整个局域网的安全配置和基于网络的攻击测试实验。这是本书的一大特色。

本教材分为基础篇、安全操作篇和攻击体会篇三篇。每篇包含若干个实验，每个实验均由“实验目的和要求”、“实验环境”、“预备知识”、“实验内容”、“实验步骤”和“实验思考”6 个部分构成。其中，“预备知识”部分对本实验所涉及的技术原理进行了清晰的讲解和陈述，使得实验的操作者能够深入理解实验的原理知识，从而做到理论与实践相结合。

基础篇由 3 个实验组成，主要介绍了实验平台的搭建方法、Windows 操作系统下涉及网络信息安全技术的相关系统命令以及对 Windows 系统进行安全配置的方法。

安全操作篇由 10 个实验组成，主要介绍了 Windows 操作系统自身的安全保障体系和基于 Windows 操作系统的安全应用协议。前者涉及 Windows 的 NTFS 文件格式、账号安全体系以及 EFS 文件加密系统等几个方面；后者涉及 FTP 文件传输、SSH、SSL 等几个方面。

攻击体会篇由 5 个实验组成，主要介绍了基于 Windows 操作系统平台的若

干攻击方法,其中包括 Windows 账号的破解、局域网的 ARP 攻击原理、远程控制机制、Windows 映像劫持原理和 SQL 注入攻击原理等几个部分。

本教材涉及的所有实验操作均在 VMWare 虚拟机上验证通过。

2. 教学指导和学习建议

本教材的目的是让学生能够了解网络信息安全的基本原理,熟练掌握网络信息安全的基本应用技能。受到教材篇幅等多方面原因的限制,我们没有对实验中所涉及的每个知识点进行深入的论述和探讨。教师可以根据学校的课程设置、教学条件和教学需要,适当增删本教程所涉及的知识点和实验操作。学生在学习本教程时,也可以根据自身的学习背景和兴趣爱好,对其中的若干实验进行深入的理论学习和研究。

本教材的每个实验均配有相应的视频资料,我们将放到清华大学出版社的网站(http://www.tup.com.cn)上供教师和学生下载参考。

3. 致谢

感谢潘金秋和黄太波两位研究生对本教程的资料搜集和视频制作所做出的贡献。

作者在本教程的编写过程中投入了大量的热情和精力,但因能力所限,难免存在疏漏之处,恳请读者批评指正。我们将虚心采纳您的意见,对教材进行不断地完善。同时,我们向所有提出批评和建议的读者表示衷心的感谢。

作　者

2012 年 1 月

CONTENTS 目录

第1篇 基础篇

第 2 篇 安全配置篇

第 3 篇 攻击体会篇

第 1 篇

基 础 篇

ARTICLE 1

实验1 实验环境建设

1.1 实验目的与要求

- 掌握虚拟机的基础知识。
- 掌握安装 VMware 的方法。
- 掌握使用 VMware 搭建局域网实验环境的方法。

1.2 实验环境

- Windows XP 系统的 PC 一台。
- VMware Workstation 5.5 安装软件。

1.3 预备知识

通过虚拟机技术,可以在一台 PC 上安装多种操作系统,模拟多个 PC 的同时运行,还可以将这些模拟出来的 PC 组成一个网络。目前主流的 x86 虚拟技术有虚拟硬件模式和虚拟软件模式两类。

1. 虚拟硬件模式

虚拟硬件模式是最初的虚拟机模式,它起源于 IBM 大型机的逻辑分区技术,该技术的特点是:每一个虚拟机都是一台真正计算机的完整副本,一个功能强大的主机可以被分割成许多虚拟机。

虚拟硬件模型在计算机、存储设备和网络硬件间建立了一个抽象的虚拟化平台,使得所有的硬件被统一到一个虚拟化层,通过使用该虚拟化层,可提供硬件级的虚拟,即虚拟机为运行于虚拟机的操作系统映像提供了一整套虚拟的 Intel x86 兼容硬件。这套虚拟硬件虚拟了真正服务器所拥有的全部设备:主板芯片、CPU、内存、SCSI 和 IDE 磁盘设备、各种接口、显示和其他输入输出设备。并且,每个虚拟机都可以被独立地封装到一个文件中,能够实现虚拟机的灵活迁移。同时,在该模式中每个用户都可以在虚拟机上执行各种操作,包括运行程序、存储数据,当虚拟机崩溃时,系统本身和其他系统用户不会受到任何影响,这表明虚拟机不仅允许资源共享,还实现了系统资源的保护。

虚拟硬件技术有以下两个主要特点：

(1) 可以直接用系统处理器执行 CPU 指令，根本涉及不到虚拟层。

(2) 实现真正的分区隔离，每个分区只占用一定的系统资源，包括磁盘 I/O 和网络带宽，并提高了系统的整体安全性。

另外，高端的虚拟服务器产品可以直接在硬件上运行虚拟机，而不需要宿主操作系统。并且，通过相关的管理软件，可以对每个虚拟机消耗的物理资源(网络带宽、磁盘 I/O 访问等)进行精确的控制。

2. 虚拟软件模式

虚拟操作系统模式是在虚拟机运行的主机操作系统之上创建了一个虚拟层，在该虚拟层之上，能够创建多个相互隔离的虚拟专用服务器(Virtual Private Server，VPS)。这些 VPS 能以最大化的效率共享硬件、软件许可证以及管理资源。对其用户和应用程序来讲，每一个 VPS 平台的运行和管理都与一台独立主机完全相同，因为每一个 VPS 均可独立进行重启并拥有自己的 root 访问权限、用户、IP 地址、内存、过程、文件、应用程序、系统函数库以及配置文件。对于运行着多个应用程序和拥有实际数据的产品服务器来说，虚拟操作系统的虚拟机可以降低成本消耗和提高系统效率。

虚拟操作系统模式同样能够满足一系列的需求：安全隔离、计算机资源的灵活性和控制、硬件抽象操作及最终高效、强大的管理功能。每一个 VPS 中的应用服务都是安全隔离的，且不受同一物理服务器上的其他 VPS 的影响。通过专用的文件系统，使得文件浏览对所有 VPS 用户来说就如常规服务器一样，但却无法被该服务器上的其他 VPS 用户看到。VPS 能够实时分配、监控、计算并控制资源级别，完成对 CPU、内存、网络输入输出、磁盘空间以及其他网络资源的灵活管理。经过抽象的 VPS 具有相同的虚拟硬件结构，并可以在任意联网的服务器之间透明迁移，而不产生任何宕机时间。

操作系统虚拟化技术解决了在单个物理服务器上部署多个生产应用服务和存储服务器时所面临的挑战。在应用服务部署完成之后，它们被集中于同一种操作系统以便于管理和维护。操作系统虚拟化是针对生产应用和服务器的完美虚拟化解决方案，共享的操作系统提供了更为有效的服务器资源并且大大降低了处理损耗。通过操作系统虚拟化，上百个 VPS 可以在单个的物理服务器上正常运行。

然而，这种集中于同一操作系统的特性使得该类虚拟机只能在同一台物理服务器上运行同一种虚拟的操作系统，比如，不能够同时运行虚拟的 Windows 和 Linux 系统。

VMware 公司是全球领先的虚拟技术开发厂商。其解决方案通过采用硬件虚拟化技术，将操作系统与应用软件分离，可显著提高系统的工作效率、可用性和灵活性。目前 VMware 公司主要有 3 种产品：VMware Workstation、VMware Infrastructure 与 VMware VMotionTM。本实验教材搭建实验平台所采用的虚拟化工具是 VMware Workstation 5.5。该产品有以下特点：

(1) 可以将已有的虚拟机文件直接进行移植，提高工作效率。

(2) 多个虚拟机可同时、独立运行，一个虚拟机崩溃不会影响其他虚拟机的正常运行。

(3) 虚拟机提供多种网络接入方式，可以直接访问外网，也可以将多个虚拟机组成虚拟机组，形成一个局域网。

(4) 提供 VMware-tools 工具,可增强虚拟操作系统图像显示和鼠标操作的功能。

(5) 具有 Team 功能,即可以在 VMware 平台上安装多个虚拟操作系统,并将这些操作系统组成一个 Team,以便形成一个局域网环境。

1.4 实验内容

本章的实验内容包括以下两个部分:(1)演示如何在 Windows 环境下安装 VMware Workstation 5.5 软件。(2)演示如何在 VMware 平台上创建一个包含多种虚拟 Windows 操作系统(包括 Windows 2000、Windows 2003 Server、Windows XP 等)的 Team,并进行配置,以便在单台计算机上构建出一个虚拟的局域网环境。该局域网环境能够满足本书所有实验所需的实验条件。

1.5 实验步骤

1.5.1 虚拟机的安装

1. 安装 VMware Workstation 5.5

单击 VMware Workstation 5.5 安装文件,启动 VMware 虚拟机的安装过程。在 Configure Product 安装界面中,选中 Yes disable autorun 复选框,将 CD-ROM 的自动运行功能关闭,以避免安装出现错误(重启机器后,自动运行功能自动打开),如图 1.1 所示。

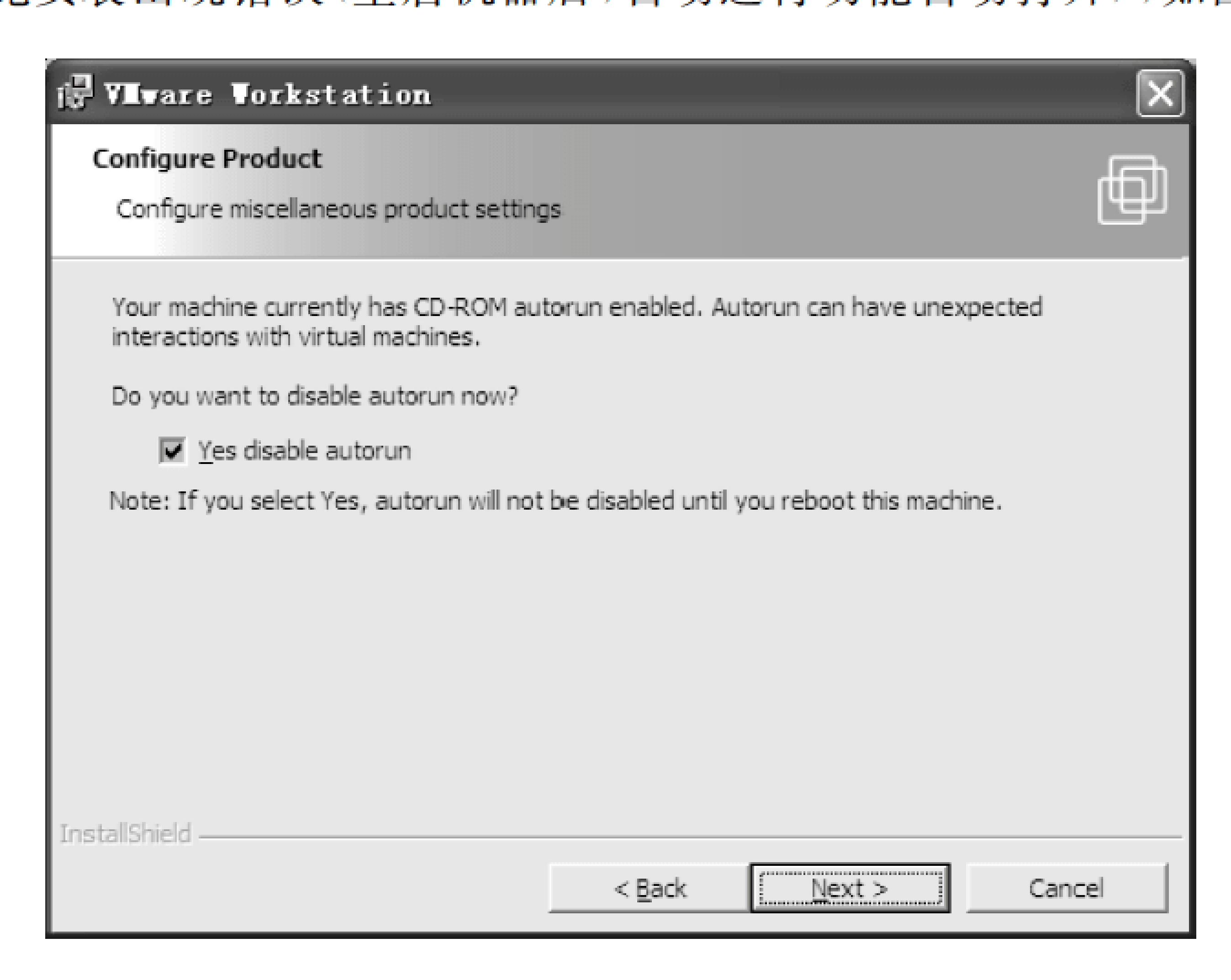


图 1.1 关闭 CD-ROM 的自动运行过程

单击 Next 按钮,按照提示继续软件的安装过程,如图 1.2 所示。

单击 Finish 按钮,完成软件的安装,如图 1.3 所示。

至此,VMware Workstation 顺利安装完成。

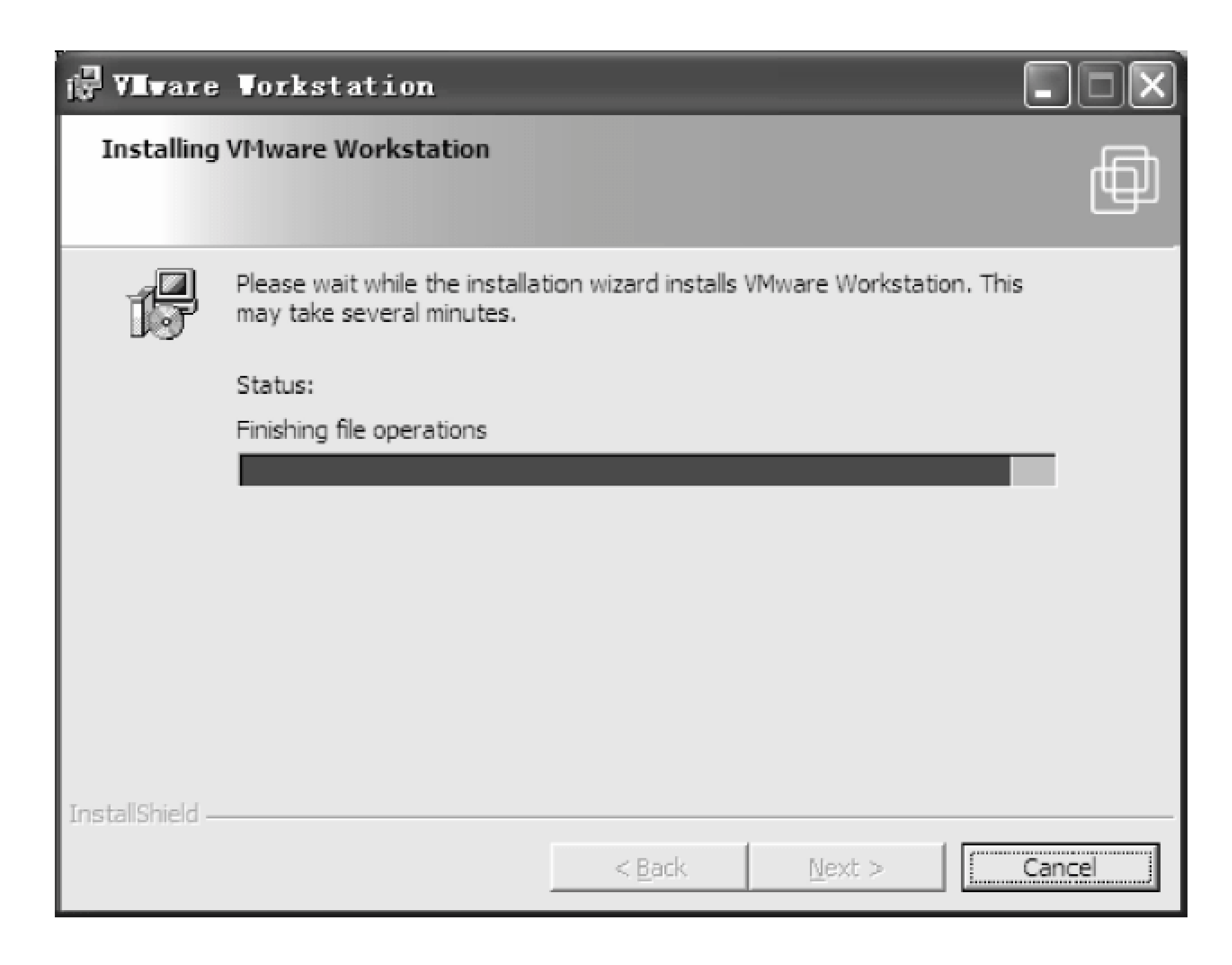


图 1.2 VMware Workstation 安装过程



图 1.3 VMware Workstation 安装完毕

2. 安装虚拟机

打开 VMware Workstation 软件，开始进行虚拟的安装，如图 1.4 所示。

首先选择菜单 File→New→Virtual Machine，激活新虚拟机的创建界面，如图 1.5 所示。

单击"下一步"按钮，选择新建虚拟机的配置，如图 1.6 所示。其中 Typical 选项为默认选项，能够创建一个具备常用配置和常用设备的虚拟机。如果 Typical 选项不能满足用户需求，则可以通过 Custom 选项创建自定义配置和能够满足特定硬件兼容需求的虚拟机。在本实验中，采用 Typical 选项创建虚拟机。

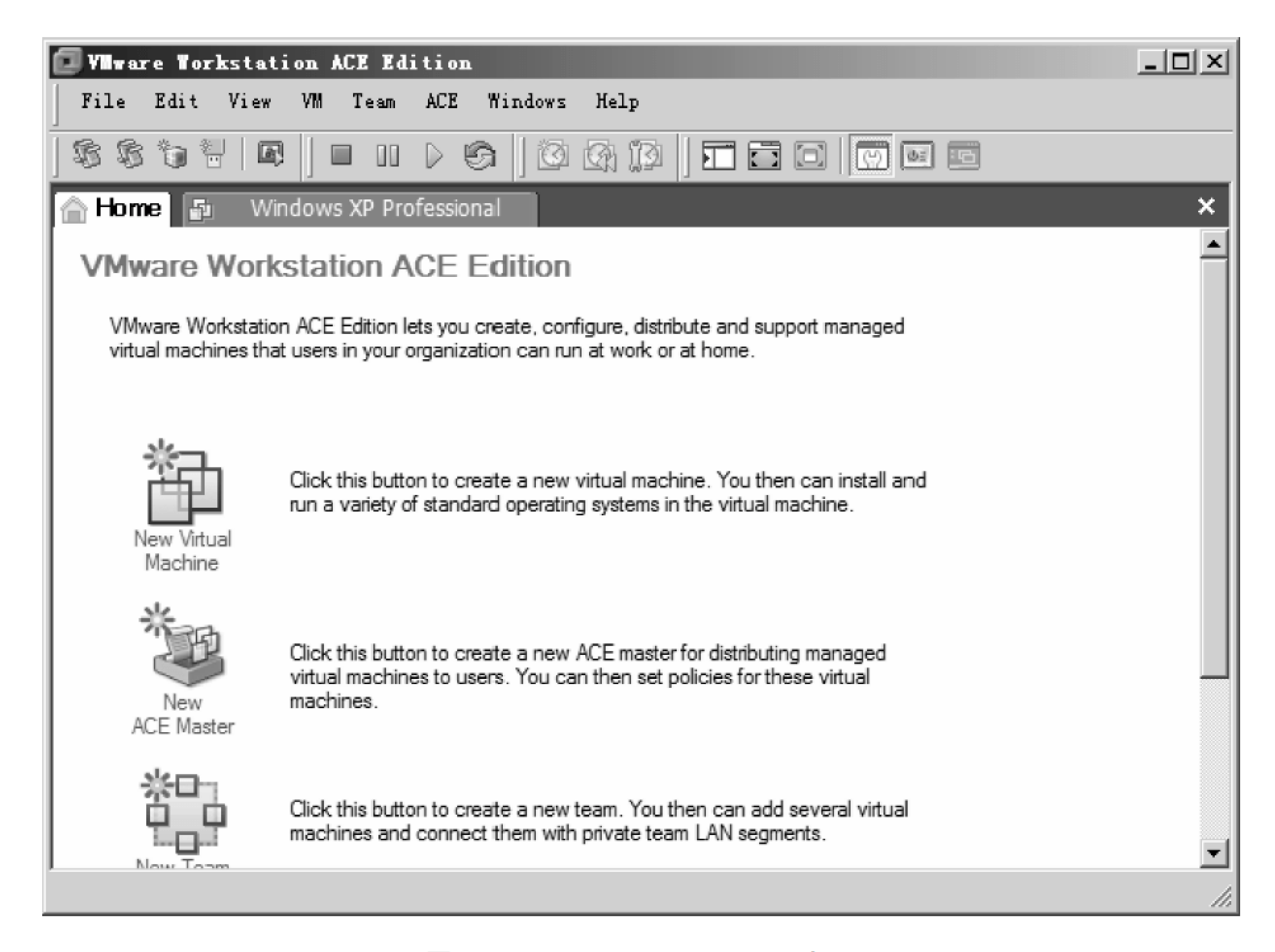


图 1.4　VMware Workstation 窗口



图 1.5　虚拟机的创建界面

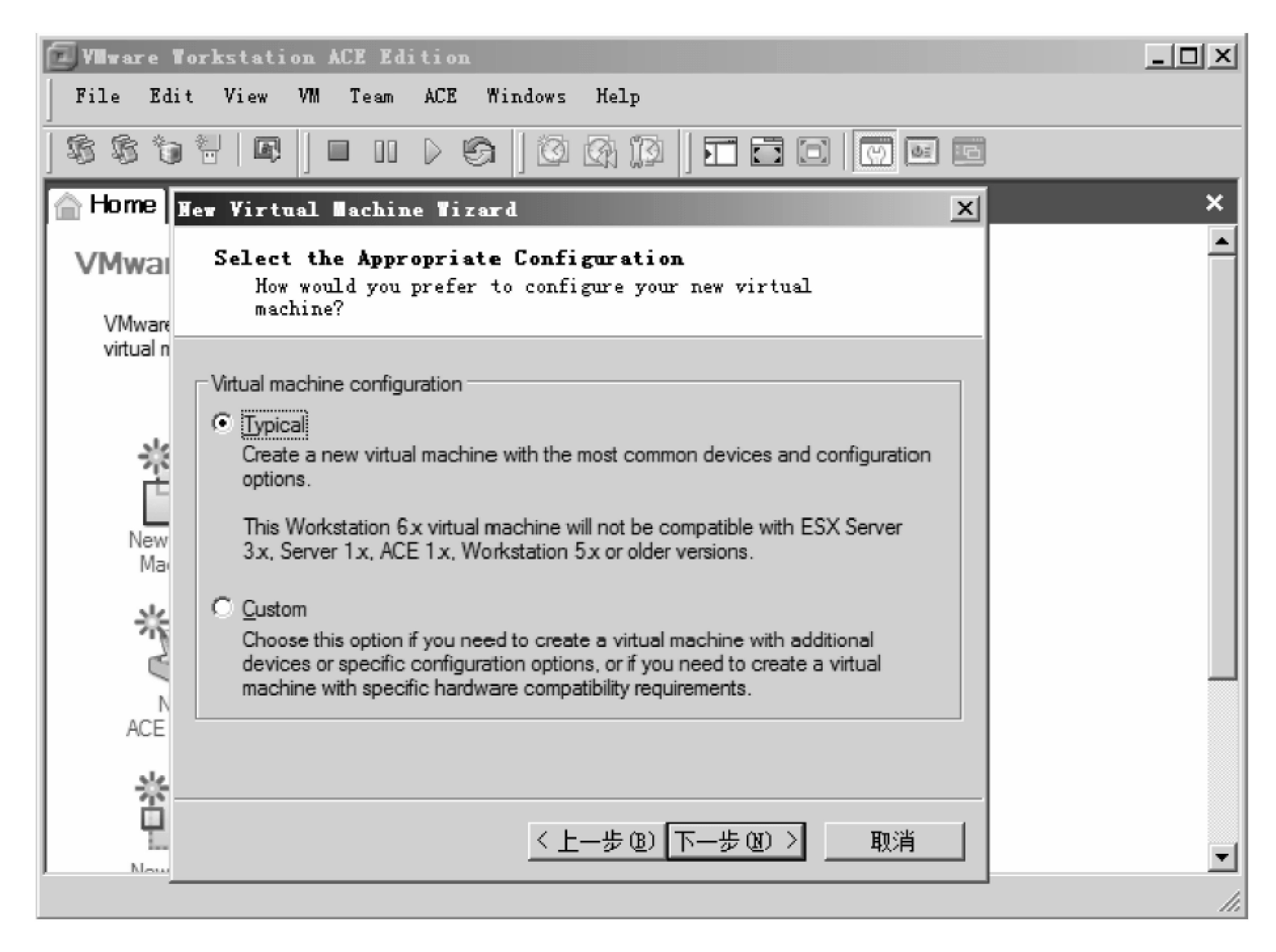


图 1.6 虚拟机配置

单击“下一步”按钮,选择所创建的虚拟机的类别和型号,如图 1.7 所示。

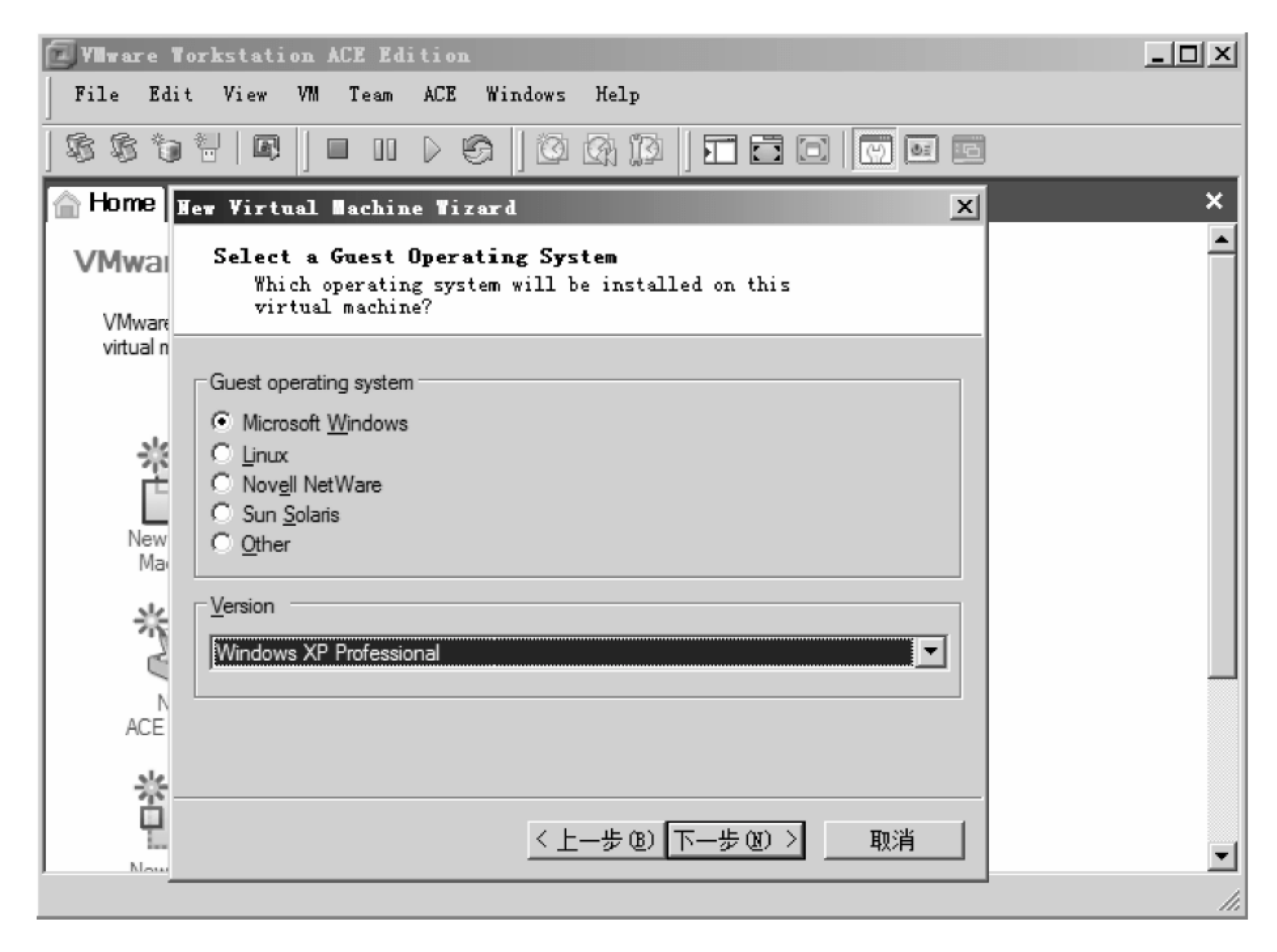


图 1.7 选择虚拟机的类别和型号

单击“下一步”按钮，可以自定义所创建的虚拟机文件的文件名，并可自定义虚拟机文件，如图1.8所示。

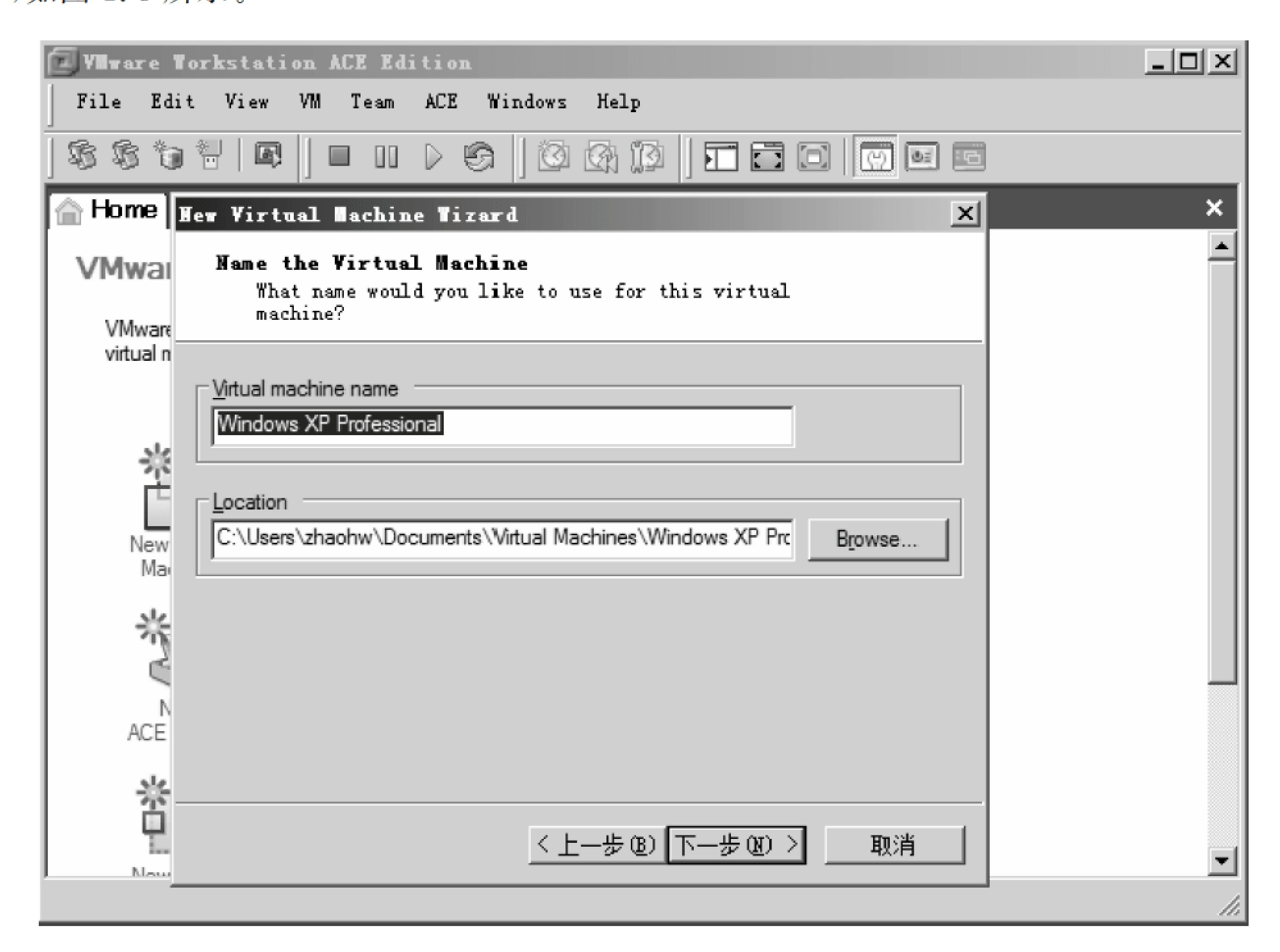


图1.8 定义虚拟机文件

单击“下一步”按钮，则可以配置虚拟机的网络类型，如图1.9所示。第1种为桥接模式(use bridged networking)，在该模式下，可以为虚拟机指定一个外网IP地址，则虚拟机利用该IP地址能够直接上网；第2种为网络地址转换模式(NAT)，在该模式下，虚拟机首先连接到主机，然后利用主机的IP地址上网；第3种为主机模式，在该模式下，虚拟机可以连接到主机的私有虚拟网；第4种为无网络模式，即虚拟机无网络连接。

注：*虚拟机的网络配置也可以在虚拟机安装完成后设置。*

单击“下一步”按钮，设置虚拟机的硬盘大小，如图1.10所示。在设置该参数时，一定要考虑主机硬盘的容量。

单击“完成”按钮，则完成了虚拟机的参数设置。

接下来，需要将Windows的安装盘装入光驱，以便安装指定的Windows操作系统。步骤略。

当指定的操作系统安装完毕后，仍然可以对虚拟机所挂接的设备参数进行调整，如图1.11所示。

例如，双击图1.11右下方的Devices栏中的Memory，则会弹出Memory对话框，在该对话框中，可以对虚拟机的内存进行重新调整，如图1.12所示。

当单击图1.11中工具栏的三角按钮时，则可以启动已安装的Windows操作系统。



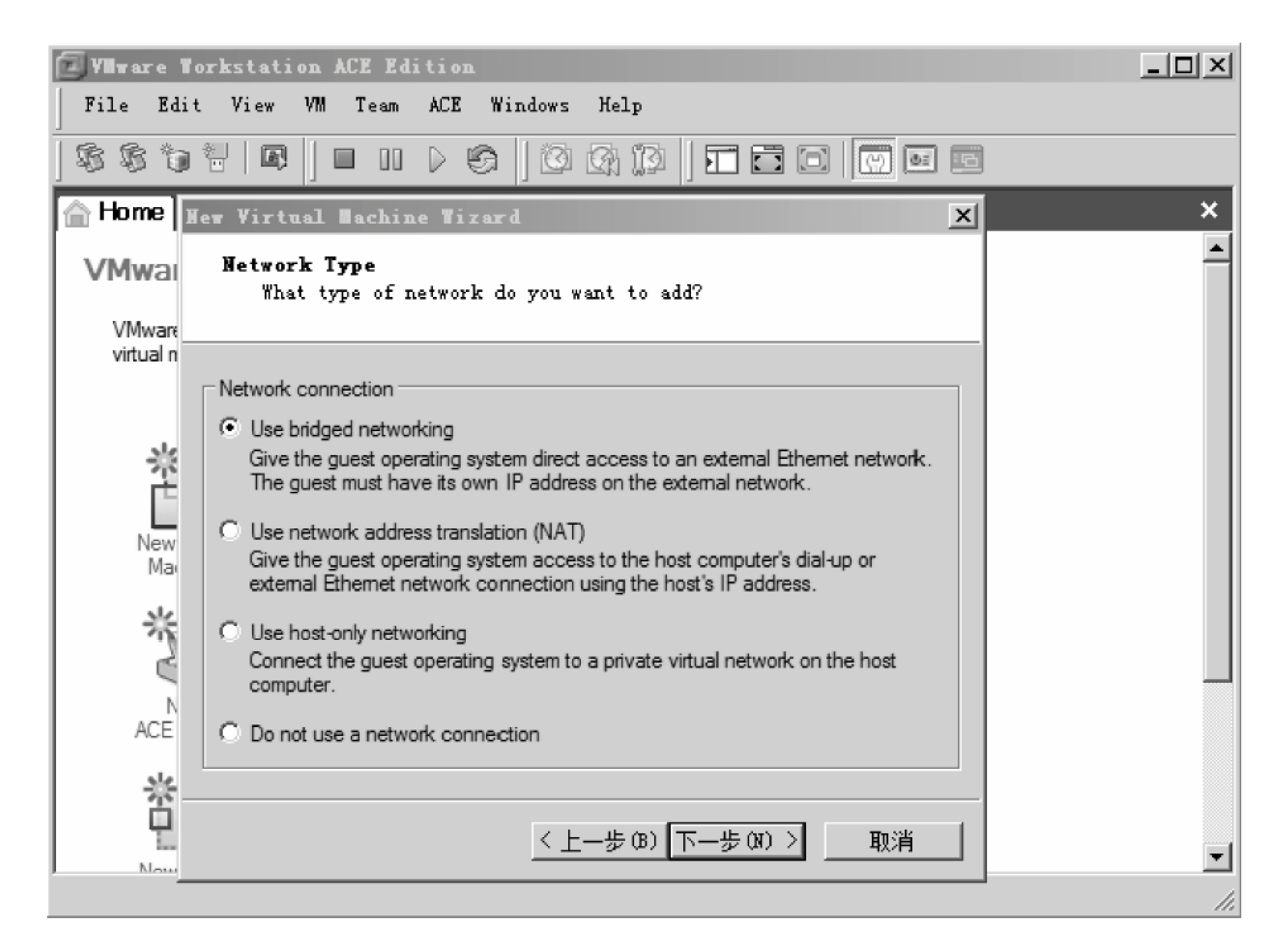


图 1.9 虚拟机的网络配置

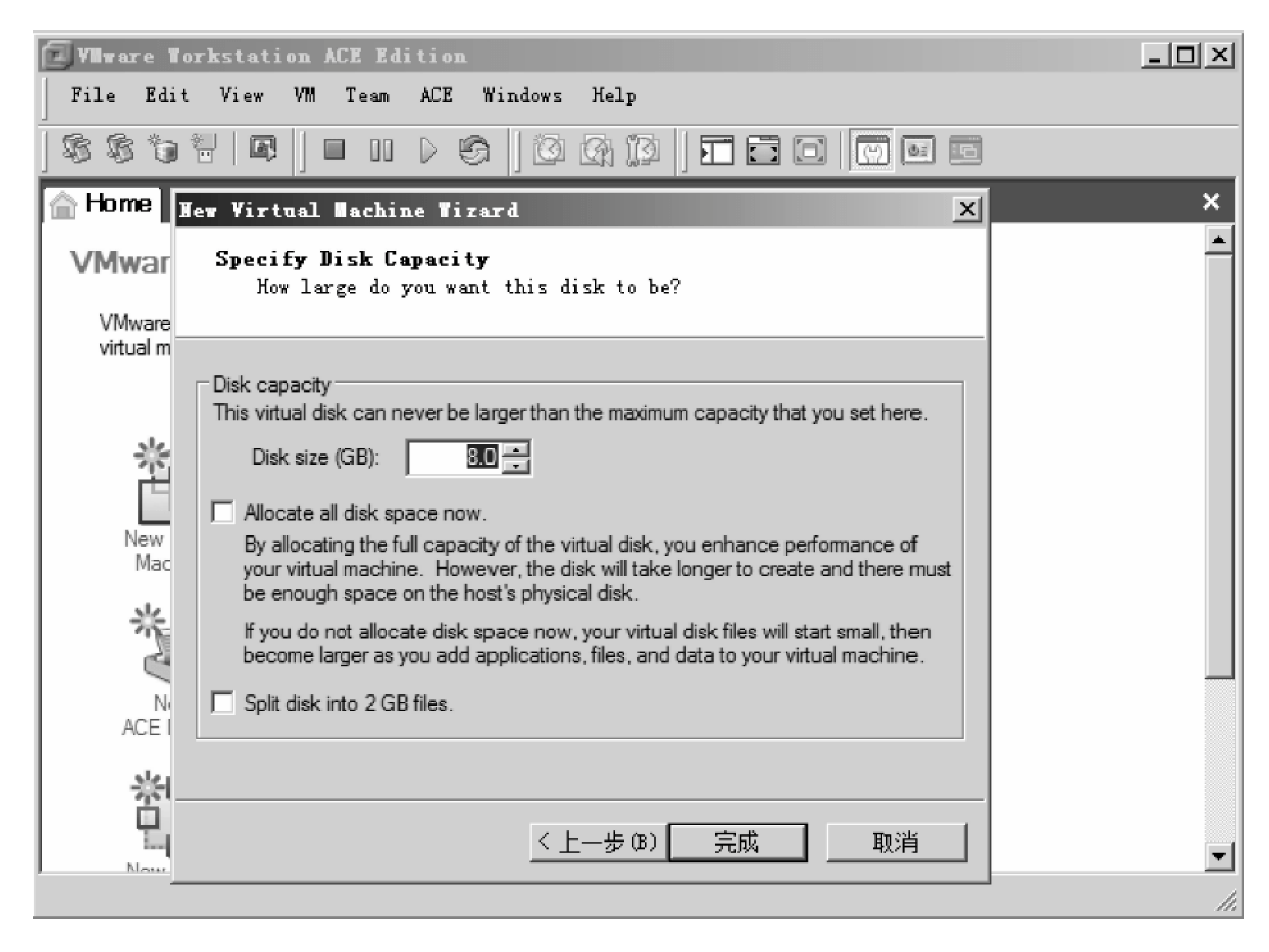


图 1.10 设置虚拟机硬盘大小

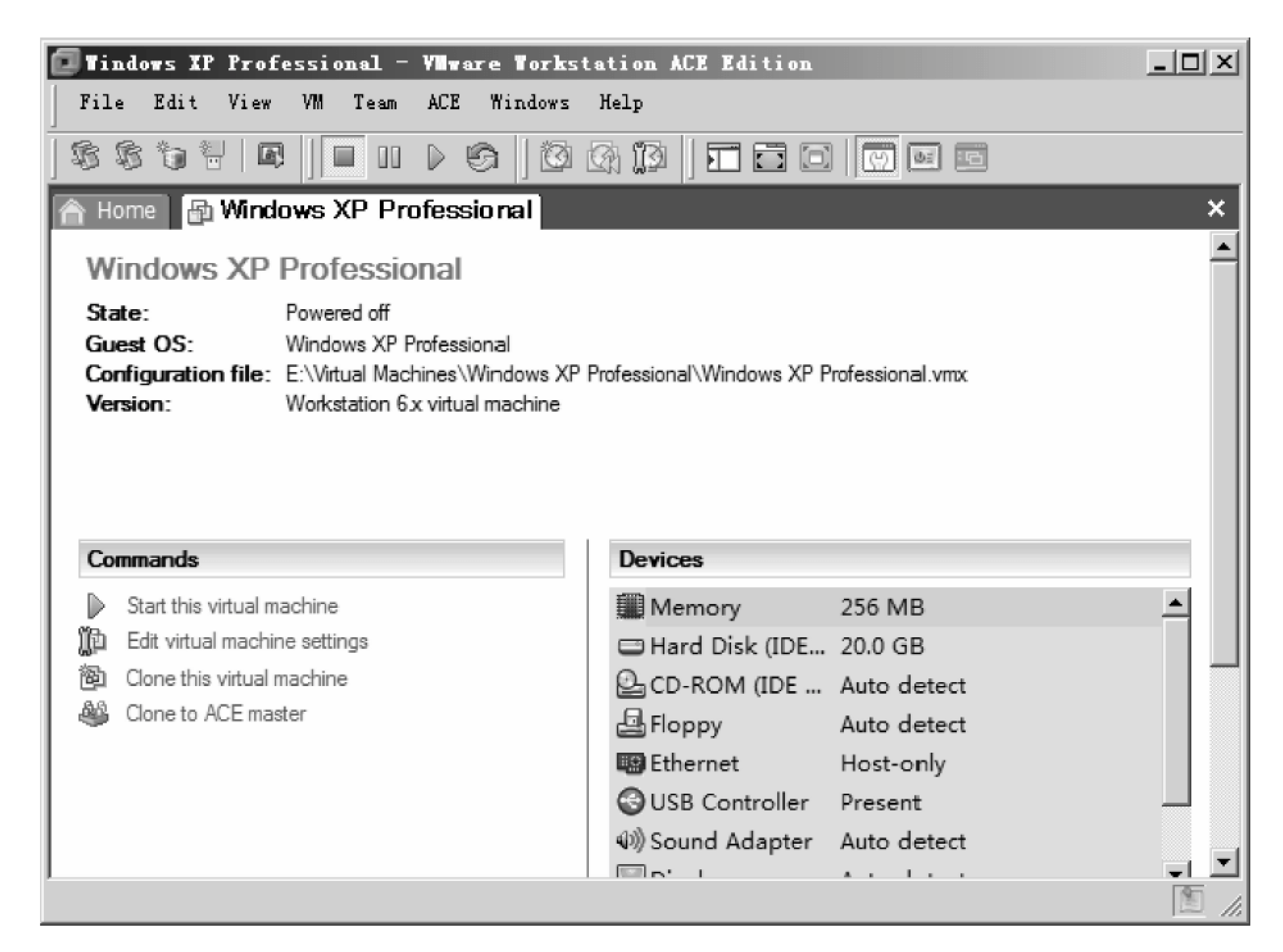


图 1.11 安装后的虚拟机

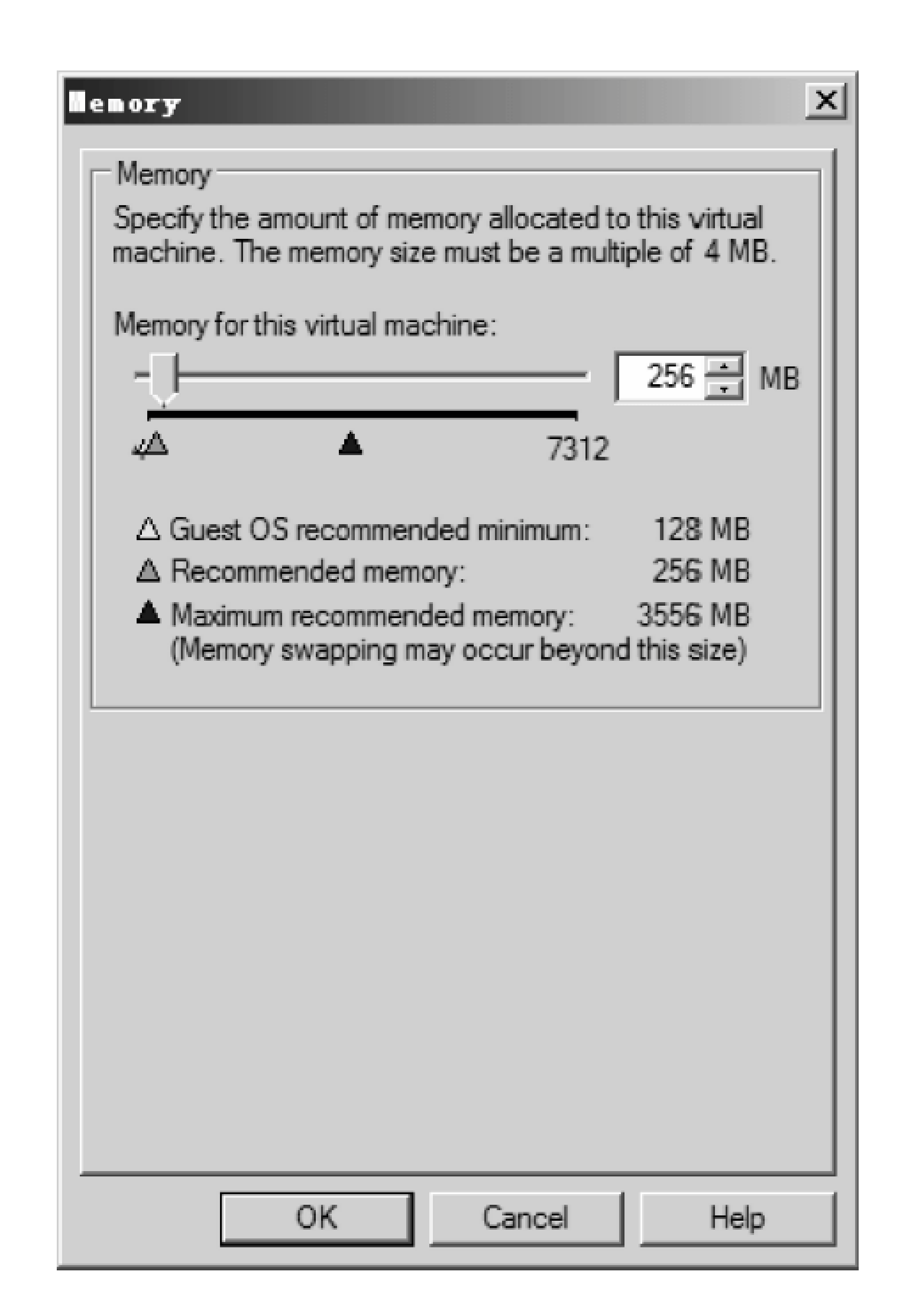


图 1.12 内存调整

1.5.2 Team 的安装

在本书的实验体系中，多个实验需要网络环境的支持。为了满足这些实验的要求，需要在 VMware 中安装多个虚拟机，并将这些虚拟机加入到一个 Team 中，以便形成一个局域网环境。下面进行 Team 的设置。

首先选择菜单 File→New→Team，进入 Team 的设置环节，如图 1.13 所示。



图 1.13 Team 的设置

单击“下一步”按钮，设置 Team 文件的名称和 Team 文件的保存位置，如图 1.14 所示。

单击“下一步”按钮，则进入将虚拟机加入 Team 的过程。在图 1.15 中，单击左下方的 Add 按钮，在弹出的下拉菜单中选择 Existing Virtual Machine，在弹出的文件管理窗口中选择一个指定的虚拟机文件，如图 1.16 所示。

在图 1.16 中，选中一个已有的虚拟机文件，并单击“打开”按钮，则将该虚拟机文件对应的虚拟机加入到了 Team 中。

单击图 1.15 中的“下一步”按钮，则可以为 Team 设置一个局域网环境，在图 1.17 中，有 3 种选项可使得一个虚拟机加入 Team 组成的网络：LAN1、Bridged 和 NAT。在这里选中 LAN1 模式即可(注：这 3 种网络配置可以在任何时间下，通过系统菜单 Team→Setting menu 进行修改)。

上述步骤操作完成后，当启动 Team 时，Team 中的所有虚拟操作系统将同时开启。当这些虚拟操作系统分别登录后，则会形成一个局域网络，为后续的实验所使用。

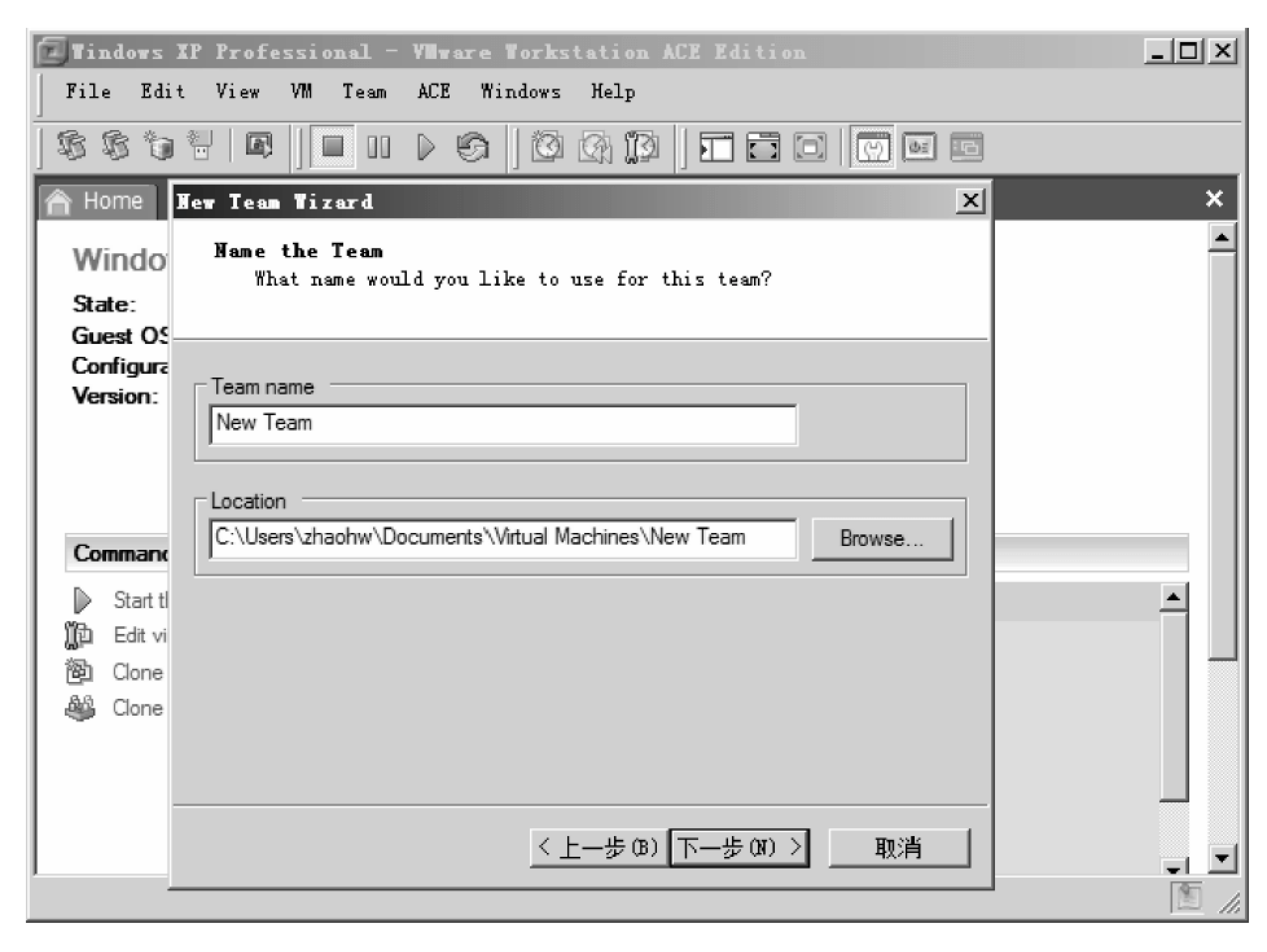


图 1.14 设置 Team 文件

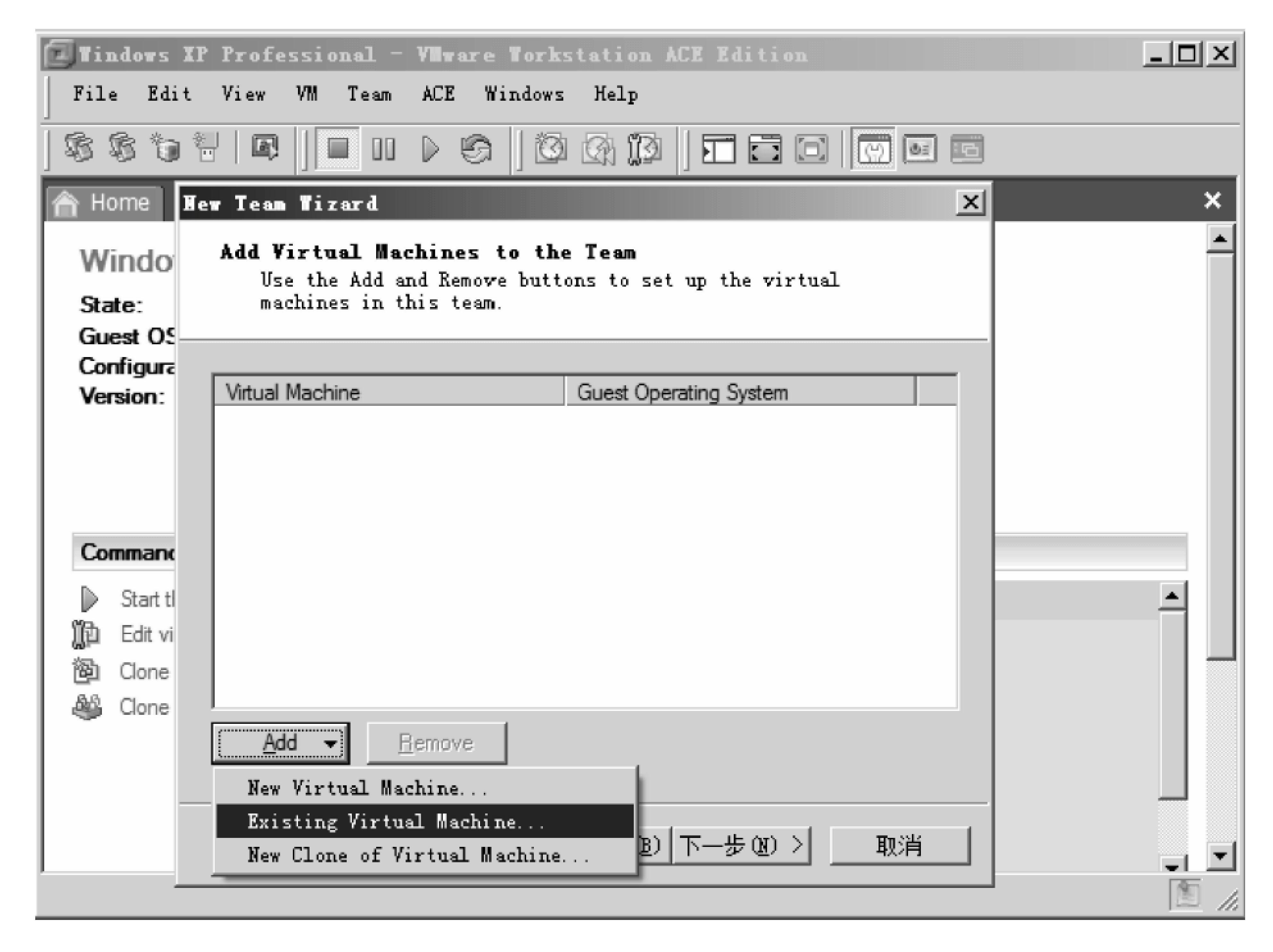


图 1.15 通过已有虚拟机文件配置 Team

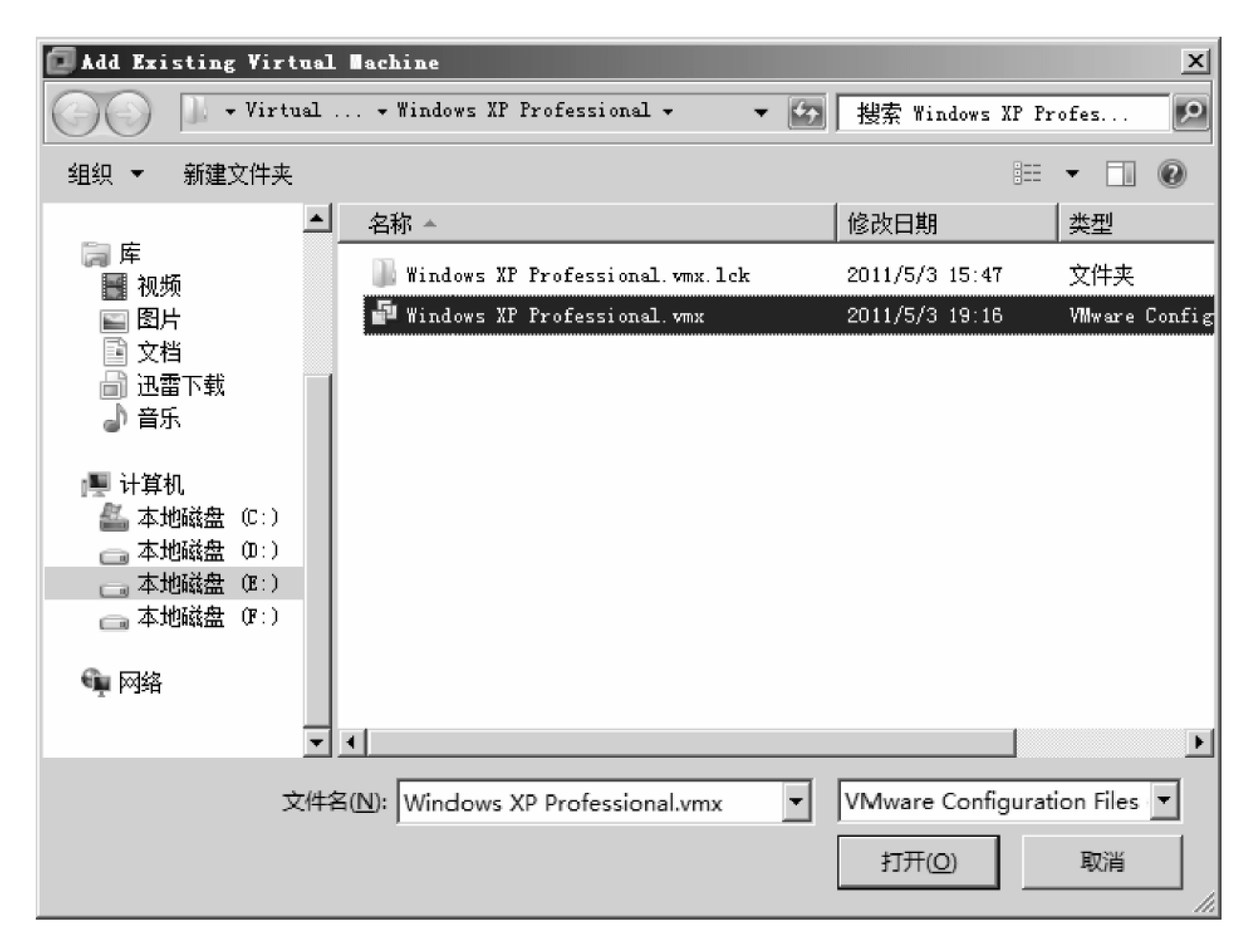


图 1.16 选择已安装的虚拟机文件

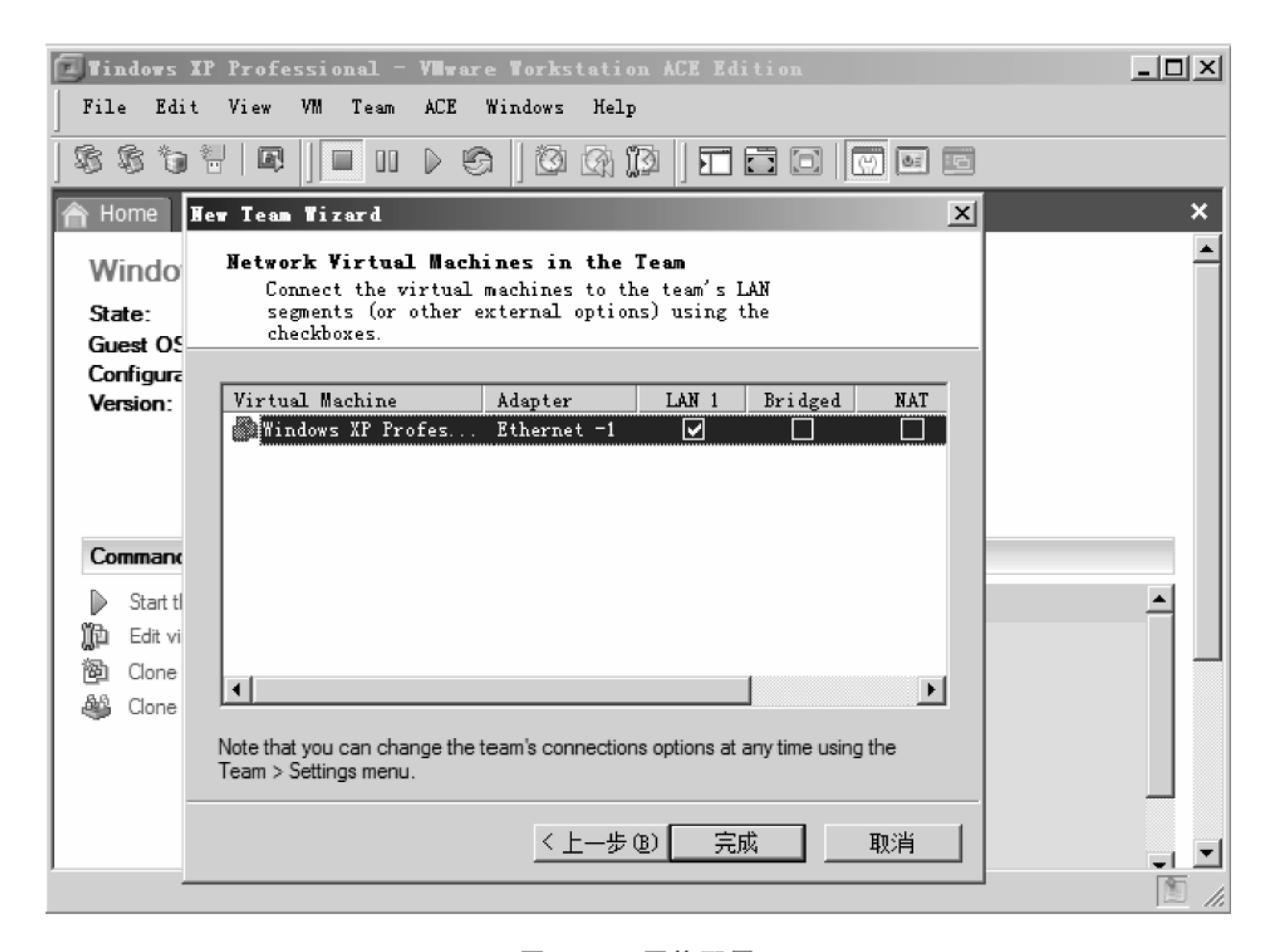


图 1.17 网络配置

1.6 实验思考

（1）请查阅相关资料，探究 Team 中的 3 种网络配置方法（LAN1、Bridged 和 NAT）各自的功能。

（2）请查阅相关资料，研究如何才能在虚拟操作系统和主机操作系统之间实现文件的直接复制和粘贴。

实验2 常见的系统命令

2.1 实验目的与要求

掌握常见的系统命令。

2.2 实验环境

- 有网络连接的 PC 一台。
- 安装有 TCP/IP 协议的 Windows 操作系统。

2.3 预备知识

在 Windows 系统中，可以通过鼠标单击的方式进行文件的打开/关闭、程序的执行/终止，这种图形界面的操作方式直观、简单，被人们所熟知。除此之外，Windows 系统还提供了另外一种操作手段，即人们可以在命令行窗口中通过输入 DOS 命令来对系统进行操作。尽管这种操作方式在对文件和程序进行操作时较为繁琐，但在某些情况下，特别是在对系统的网络环境进行配置和管理时，却体现出独特的优势，甚至能够完成通过鼠标单击无法完成的功能。

2.4 实验内容

本章的实验内容主要演示命令行环境的开启以及 Ping、Nbtstat、Netstat、Tracert 和 Net 命令集等命令的各个参数的功能和使用方法。灵活使用这些命令及相关参数不仅可快速查看本地局域网和当前计算机网络环境的状态，并能够进行相应的网络配置。

2.5 实验步骤

1. 启动命令行窗口

在 Windows 2000/2003 或 Windows XP 系统中，单击“开始”→“运

行”命令，在弹出的“运行”对话框中输入 CMD 命令，单击“确定”按钮后进入命令行环境，如图 2.1 所示。



图 2.1 启动命令行窗口

2. 使用 Ping 命令

Ping 命令是用来检查网络是否通畅或者网络连接速度的命令，该命令利用如下的原理：网络上的每台机器都有唯一确定的 IP 地址，我们给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的信息，就能确定目标主机是否存在，并进一步判断出目标主机的操作系统等信息。

在命令行窗口中输入 Ping 命令，则能得到有关 Ping 命令的用法介绍，如图 2.2 所示。

```
命令提示符

C:\Documents and Settings\Administrator>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.


C:\Documents and Settings\Administrator>_
```

图 2.2 Ping 命令用法

其中，参数“-t”表示将不间断地向目标 IP 发送数据包，直到强制终止其运行(按 Ctrl+C 组合键进行终止)，如图 2.3 所示。

```
命令提示符
C:\Documents and Settings\Administrator>ping -t 192.168.1.104

Pinging 192.168.1.104 with 32 bytes of data:

Reply from 192.168.1.104: bytes=32 time=7ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time=3ms TTL=128
Reply from 192.168.1.104: bytes=32 time=4ms TTL=128
Reply from 192.168.1.104: bytes=32 time=3ms TTL=128
Reply from 192.168.1.104: bytes=32 time=3ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.104:
    Packets: Sent = 19, Received = 19, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

图 2.3　-t 参数的使用

参数“-l”定义发送数据包的大小，默认为 32 字节，利用它可以最大定义到 65 500 字节，如图 2.4 所示。

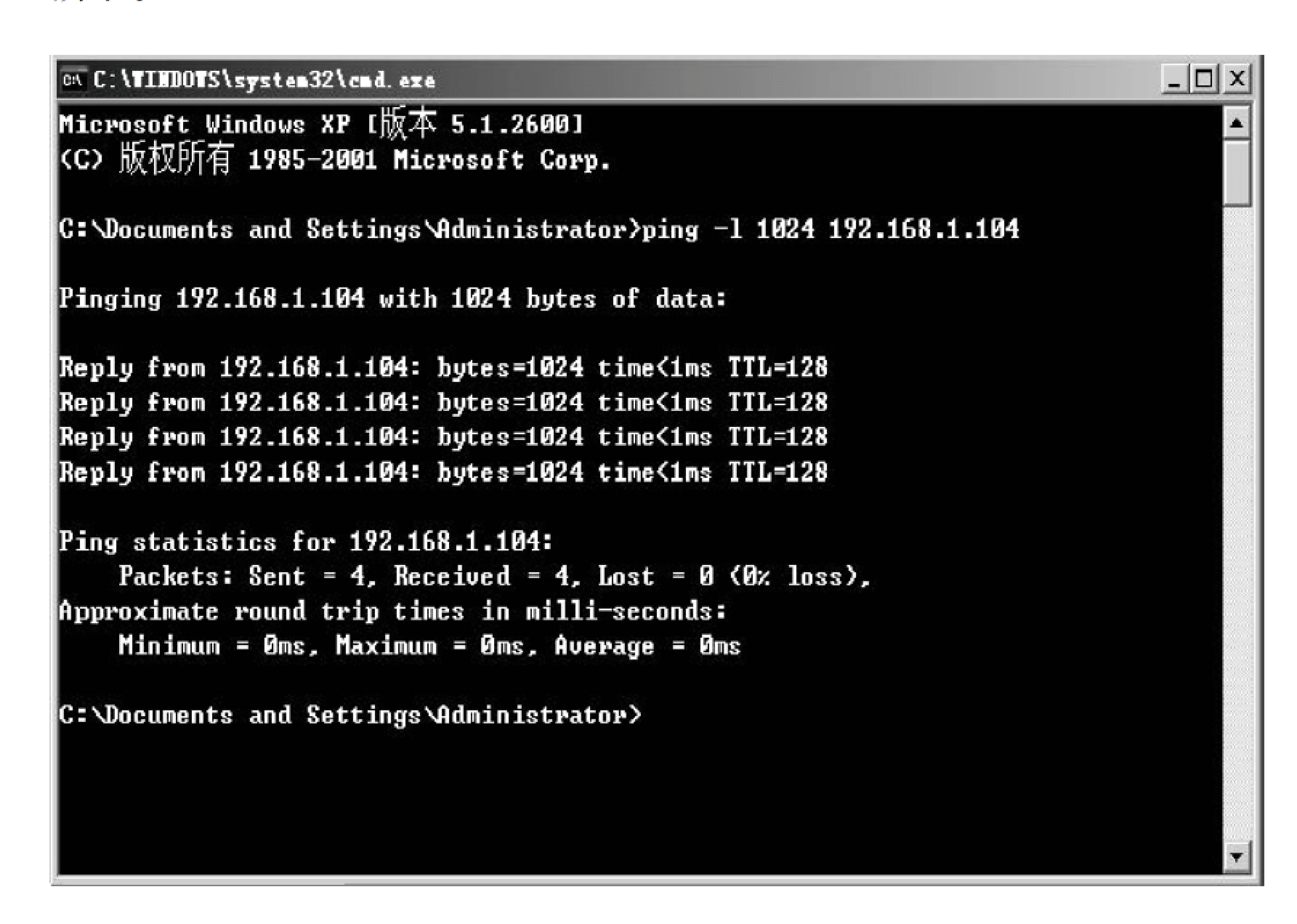
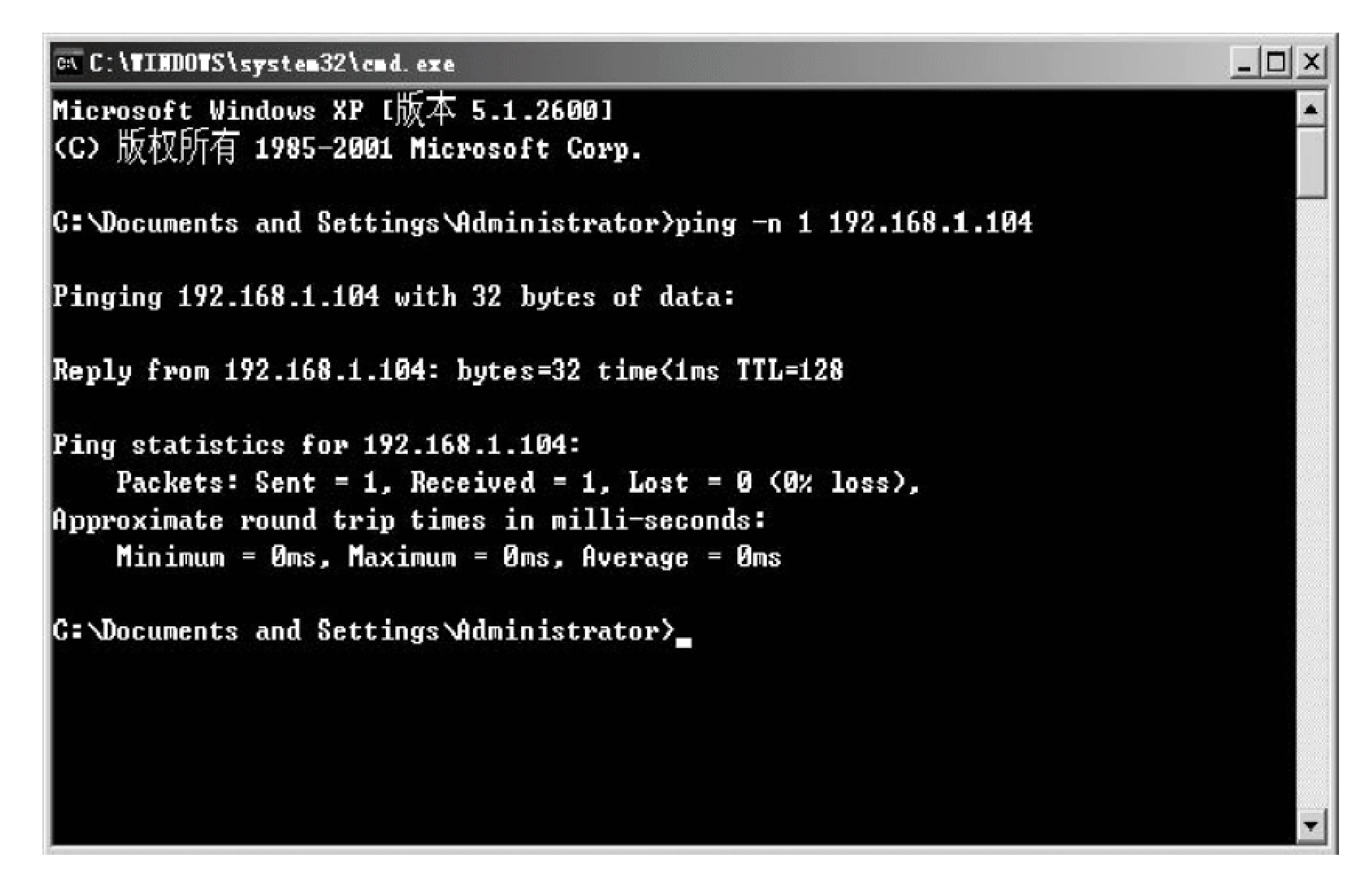


图 2.4　-l 参数的使用

参数“-n”定义向目标 IP 发送数据包的次数,默认为 3 次。如果网络速度比较慢,定义 1 次即可,如图 2.5 所示。


C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping -n 1 192.168.1.104

Pinging 192.168.1.104 with 32 bytes of data:

Reply from 192.168.1.104: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.104:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

图 2.5 -n 参数的使用

在 Ping 命令返回的信息中,“时间”表示从发出数据到接收到返回数据包所花费的时间,从该参数可以判断出网络连接速度的快慢。

TTL(Time to Live,生存时间)是指数据包在网络传输的过程中,在被丢弃之前允许通过的路由器的数量。每经过一个路由器,TTL 值减 1,直至减到 0 丢弃该数据包。通过 TTL 值的计算,可以大致推算出数据包经过了多少个路由器。例如,若返回的 TTL 值为 117,则可以推算出数据包离开源地址时的 TTL 起始值为 128(即比返回 TTL 值略大的一个 2 的某个指数值,这里 $117<2^7=128$)。这样,可以推算出源地址到目标地址需要通过 11 个路由器网段。根据操作系统类型的不同,源地址的 TTL 默认起始值也不同,一般情况下,TTL=32 时,源操作系统为 Windows 98/Me; TTL=64 时,源操作系统为 Linux 或 Win 7; TTL=128 时,源操作系统为 Windows NT/2000/2003/XP; TTL=255 时,源操作系统为 UNIX。但值得注意的是,通过 TTL 的返回值来判断目标操作系统的方法并不准确,因为 TTL 的默认值是可以通过注册表修改的。

3. 使用 Nbtstat 命令

Nbtstat 命令使用 TCP/IP 上的 NETBIOS(Network Basic Input/Output System,网络基本输入输出系统)显示协议统计和当前使用 NBI(Network Binding Interface,网络关联接口)的 TCP/IP 连接。使用该命令能够得到远程主机的 NETBIOS 信息,比如用户名、所属的工作组、网卡的 MAC 地址等,从而加深对目标主机系统的认识。

为了能够使用 Nbtstat 命令,在进行实验之前,需要在“本地连接”的“属性”对话框中单击“安装”按钮,弹出“选择网络组件类型”对话框,如图 2.6 所示。在该对话框中选择“协议”,并单击“添加”按钮,然后在弹出的“选择网络协议”对话框中选择 NWLink IPX/SPX/NetBIOS Compatible Teansport Protocol 选项,如图 2.7 所示。

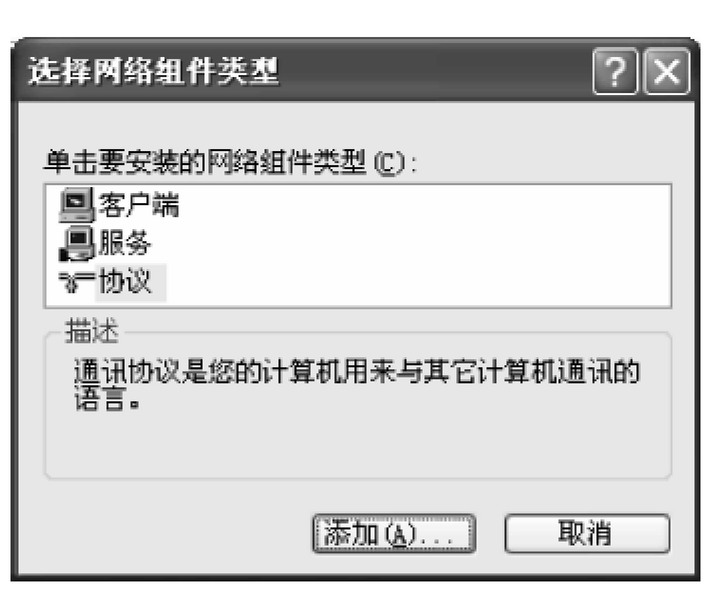




图 2.6 “选择网络组件类型”对话框



图 2.7 “选择网络协议”对话框

Nbtstat 命令的主要参数有以下几个：

- -a RemoteName　列出指定名称的远程机器的名称；
- -A IP Address　列出指定 IP 地址的远程机器的名称表；
- -c　列出远程计算机名称及其 IP 地址的 NBT(NetBIOS Over TCP/IP，基于 TCP/IP 的 NetBIOS)缓存；
- -n 列出本地的 NetBIOS 名称；
- -r 列出通过广播和经由 WINS 解析的名称；
- -S 列出具有目标 IP 地址的会话表；
- -s 列出将目标 IP 地址转换成计算机 NetBIOS 名称的会话表。

例如，在命令行中输入：nbtstat -A 192.168.1.105，则可以得到 IP 地址为 192.168.1.105 的计算机的名称表，如图 2.8 所示。

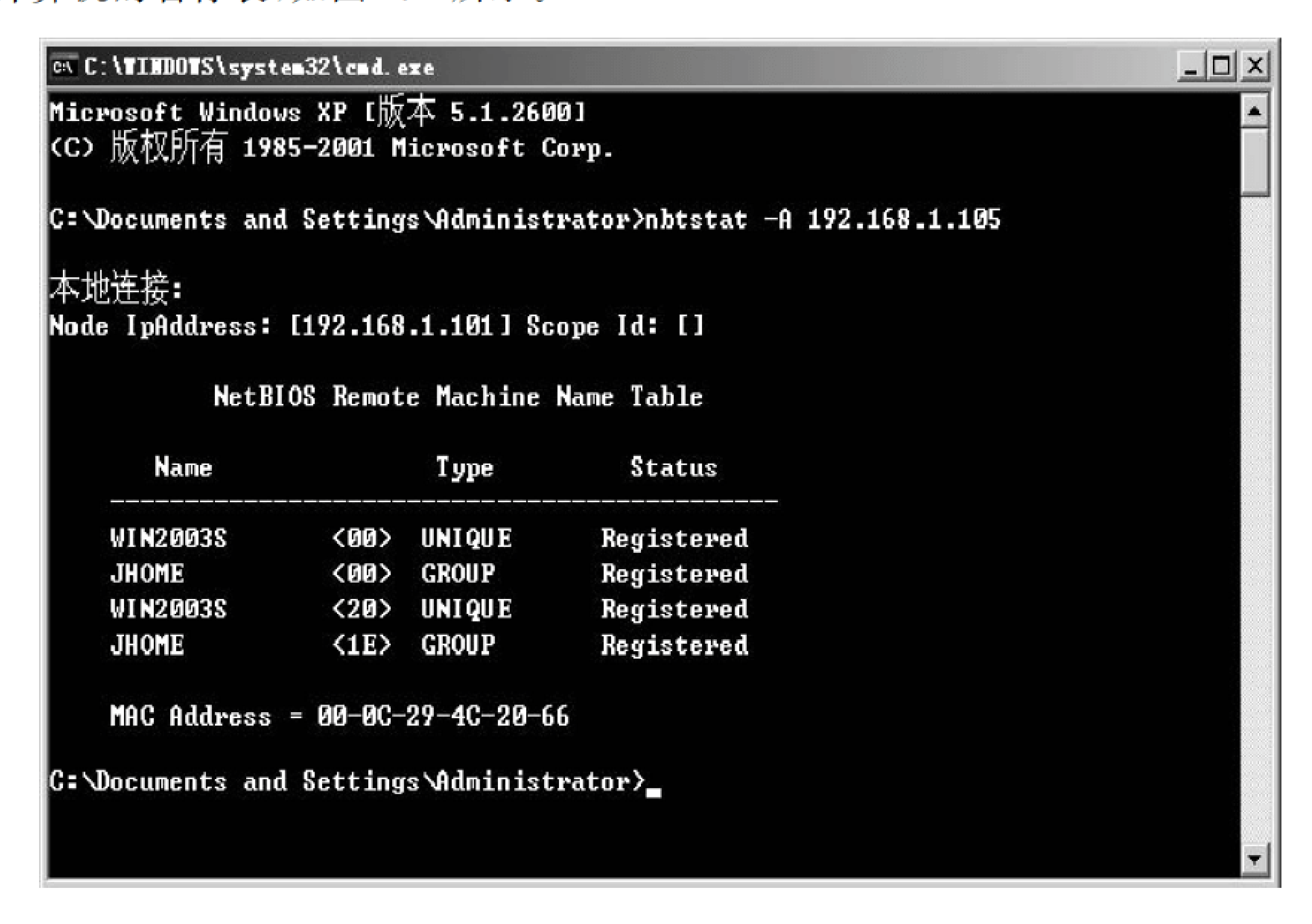


图 2.8 列出远程计算机的名称表

4. 使用 Netstat 命令

Netstat 命令可用来便捷地查看本地网络的连接状态。其中，参数“-a”能够显示所有连接和侦听端口，如图 2.9 所示。

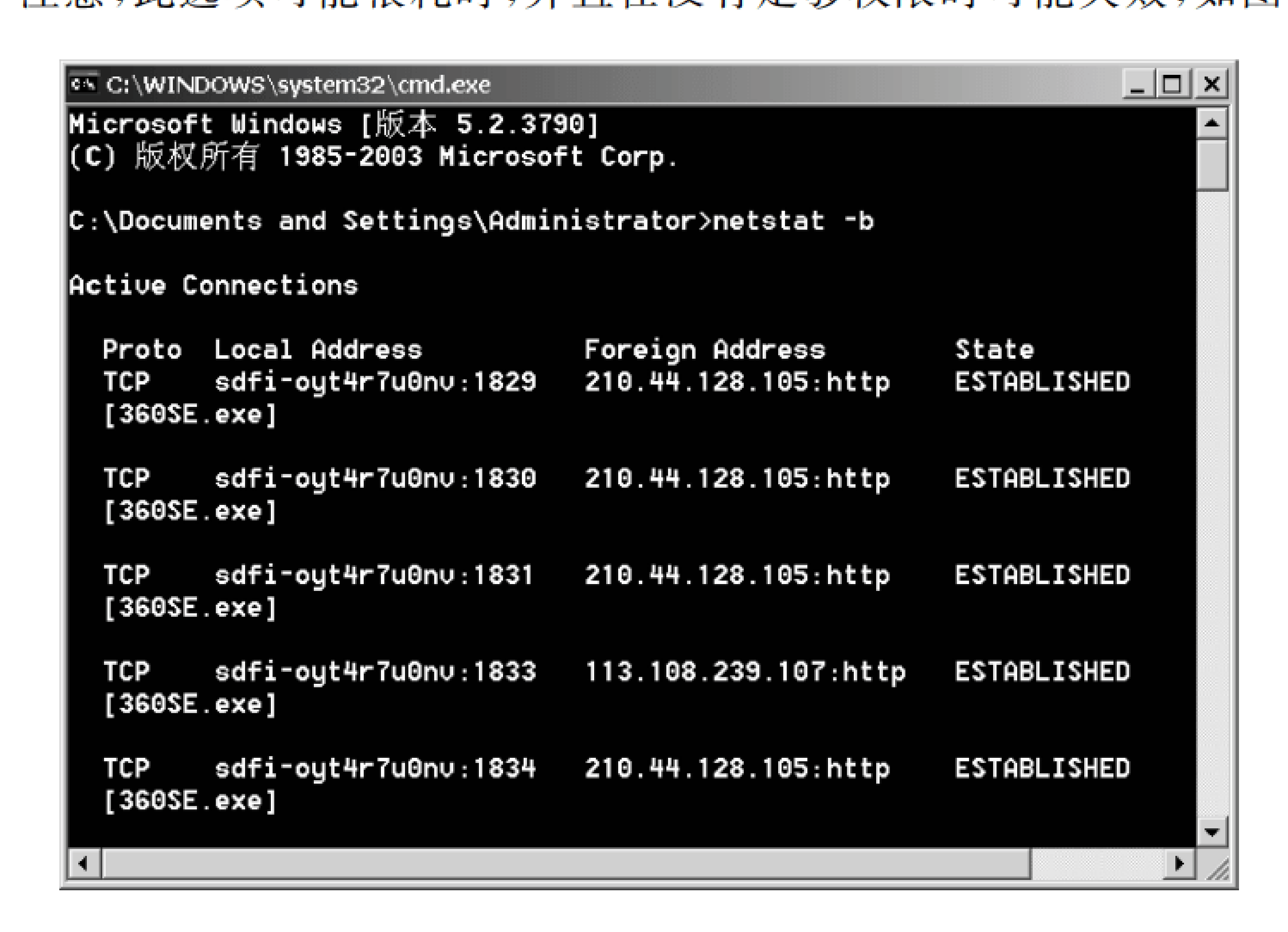
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    sdfi-oyt4r7u0nv:http   sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:pop3   sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:epmap  sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:https  sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:microsoft-ds  sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:912    sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:1025   sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:1026   sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:6001   sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:netbios-ssn  sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:netbios-ssn  sdfi-oyt4r7u0nv:0      LISTENING
  TCP    sdfi-oyt4r7u0nv:netbios-ssn  sdfi-oyt4r7u0nv:0      LISTENING
  UDP    sdfi-oyt4r7u0nv:microsoft-ds  *:*
  UDP    sdfi-oyt4r7u0nv:1042   *:*
  UDP    sdfi-oyt4r7u0nv:1735   *:*
  UDP    sdfi-oyt4r7u0nv:1737   *:*
  UDP    sdfi-oyt4r7u0nv:1738   *:*
  UDP    sdfi-oyt4r7u0nv:ssdp   *:*
```

图 2.9 -a 参数的使用

参数“-b”能够显示在创建每个连接或侦听端口时涉及的可执行程序。在某些情况下，已知可执行程序承载多个独立的组件，这些情况下，显示创建连接或侦听端口时涉及的组件序列。此情况下，可执行程序的名称位于底部方括号[]中，它调用的组件位于顶部，直至达到 TCP/IP。注意，此选项可能很耗时，并且在没有足够权限时可能失败，如图 2.10 所示。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    sdfi-oyt4r7u0nv:1829   210.44.128.105:http    ESTABLISHED
  [360SE.exe]

  TCP    sdfi-oyt4r7u0nv:1830   210.44.128.105:http    ESTABLISHED
  [360SE.exe]

  TCP    sdfi-oyt4r7u0nv:1831   210.44.128.105:http    ESTABLISHED
  [360SE.exe]

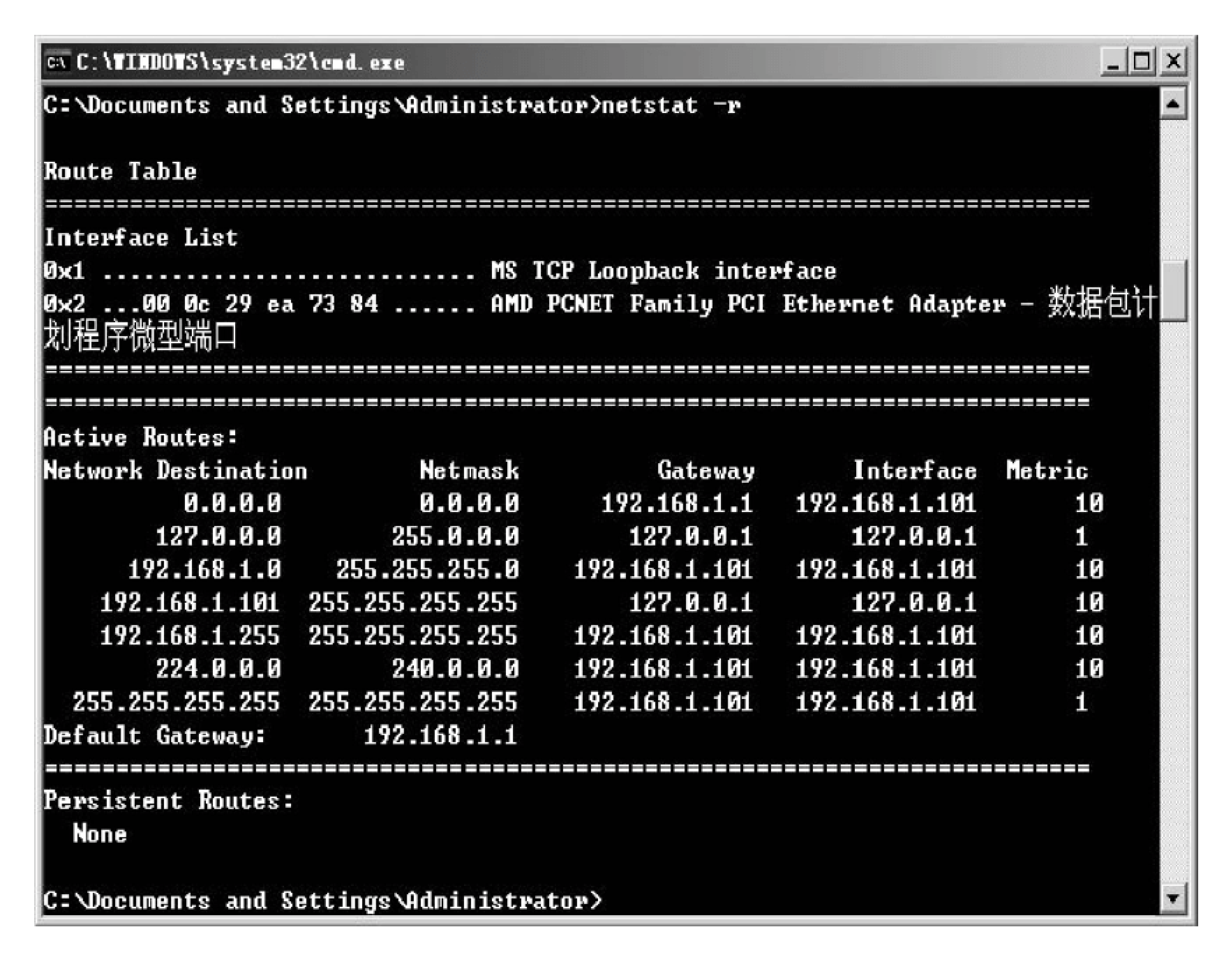
  TCP    sdfi-oyt4r7u0nv:1833   113.108.239.107:http   ESTABLISHED
  [360SE.exe]

  TCP    sdfi-oyt4r7u0nv:1834   210.44.128.105:http    ESTABLISHED
  [360SE.exe]
```

图 2.10 -b 参数的使用

参数“-r”可列出当前的路由信息，能显示本地主机的网关、子网掩码、接口列表以及路由表等详细信息。该命令的部分截图如图 2.11 所示。




```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -r

Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 ea 73 84 ...... AMD PCNET Family PCI Ethernet Adapter - 数据包计
划程序微型端口
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1   192.168.1.101       10
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.1.0    255.255.255.0    192.168.1.101   192.168.1.101       10
    192.168.1.101  255.255.255.255        127.0.0.1       127.0.0.1       10
    192.168.1.255  255.255.255.255    192.168.1.101   192.168.1.101       10
        224.0.0.0        240.0.0.0    192.168.1.101   192.168.1.101       10
  255.255.255.255  255.255.255.255    192.168.1.101   192.168.1.101       1
Default Gateway:       192.168.1.1
===========================================================================
Persistent Routes:
  None

C:\Documents and Settings\Administrator>
```

图 2.11　-r 参数的使用

5．使用 Tracert 命令

Tracert 命令可以跟踪数据包的路由信息，查询出数据包从本地机器传输到目标主机所经过的所有途经，这有助于了解网络的布局和结构，如图 2.12 所示。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>tracert www.sdfi.edu.cn

Tracing route to www.sdfi.edu.cn [210.44.128.101]
over a maximum of 30 hops:

  1     1 ms     2 ms     1 ms  210.44.134.65
  2    <1 ms    <1 ms    <1 ms  210.44.128.101

Trace complete.

C:\Documents and Settings\Administrator>_
```

图 2.12　Tracert 命令的使用

图 2.11 说明数据从本地计算机连接到 www. sdfi. edu. cn 所在的主机时，中间经过了一次中转。

Tracert 命令的主要参数如下：

- -d　不将地址解析成主机名；
- -h maximum_hops　搜索目标的最大跃点数；
- -j host-list　与主机列表一起的松散源路由（仅适用于 IPv4）；
- -w timeout　等待每个回复的超时时间（以毫秒为单位）；
- -R　跟踪往返行程路径（仅适用于 IPv6）；

- -S srcaddr　要使用的源地址(仅适用于 IPv6);
- -4　强制使用 IPv4;
- -6　强制使用 IPv6。

6. Net 命令集的使用

Net 命令是 Windows 系统中一种以命令行方式执行的、功能强大的网络管理命令集合,其功能包含了网络环境查询和配置、服务的开启和停止、用户账号管理以及系统登录等。熟练掌握 Net 命令集的使用能够轻松实现网络的各种管理功能。

Net 命令集中包含的各种命令如图 2.13 所示。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net
此命令的语法是:


NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]


C:\Documents and Settings\Administrator>
```

图 2.13　Net 命令集

下面对 Net 命令集中几个重要的 Net 命令进行介绍。

(1) Net accounts

Net accounts 命令可用于管理安全用户账号数据库,其功能包括修改所有账户的密码和登录请求,其实现用户登录的安全管理。

Net accounts 命令的用法如下:

```
NET ACCOUNTS [/FORCELOGOFF:{minutes | NO}] [/MINPWLEN:length]
             [/MAXPWAGE:{days | UNLIMITED}] [/MINPWAGE:days]
             [/UNIQUEPW:number] [/DOMAIN]
```

当输入不带任何参数的 Net accounts 命令时,将显示当前账户安全管理的配置情况,如图 2.14 所示。



图 2.14　Net accounts 命令的使用

其中，参数/forcelogoff:{minutes | no}用于设置当用户账号到期时，在结束用户与服务器的会话前需要等待的分钟数。No 选项能够防止强制注销。

(2) Net use

Net use 命令用于管理与远程计算机共享资源的连接，或者显示计算机贡献资源的连接情况。

Net use 命令的用法如下：

```
NET USE
[devicename | * ] [\\computername\sharename[\volume] [password | * ]]
          [/USER:[domainname\]username]
          [/USER:[dotted domain name\]username]
          [/USER:[username@dotted domain name]
          [/SMARTCARD]
          [/SAVECRED]
          [[/DELETE] | [/PERSISTENT:{YES | NO}]]
NET USE {devicename | * } [password | * ] /HOME
NET USE [/PERSISTENT:{YES | NO}]
```

当输入不带参数的 Net use 命令时，将显示当前本地计算机的连接情况。

当输入 C:\Net use \\ 192.168.1.99\ipc $ "pass" /user:"admin"命令时，则使得本地计算机能够与 192.168.1.99 建立一个 IPC $ 连接；当输入 C:\Net use z:\\192.168.1.99\C $ "aaa" /user:"bbb"命令时，将 192.168.1.99 的 C 盘影射成本地的 Z 盘。建立了 IPC $ 连接并影射后，就可以从本地机器向目标机器拷贝文件了，copy c:\test.exe z:\hack.exe 表示把本地目录下的 test.exe 传到远程主机并命名成 hack.exe。

(3) Net user

该命令用于管理、显示本地或域中计算机的用户账号信息，可以实现用户账号的添加、删除以及登录密码的修改。

Net user 命令的用法如下：

```
NET USER     [username [password | * ] [options]] [/DOMAIN]
             username {password | * } /ADD [options] [/DOMAIN]
             username [/DELETE] [/DOMAIN]
             username [/TIMES:{times | ALL}]
```

当输入不带参数的 Net user 命令时，将显示本地计算机中的用户账号，如图 2.15 所示。

当输入 net user abc 123456 /add 命令时，则会添加一个用户名为 abc，密码为 123456 的新用户账号。但需要注意的是，新添加用户的密码设置必须符合 Net accounts 命令中设置的密码规则。

当输入 net user abc /del 命令时，则会删除用户账号 abc；输入 net user abc /active:no 命令时，会将用户账号 abc 禁用；输入 net user abc 命令时，会显示有关用户账号 abc 的信息，如图 2.16 所示。

(4) Net view

该命令用于显示计算机域的列表、计算机列表或指定计算机的共享资源列表。

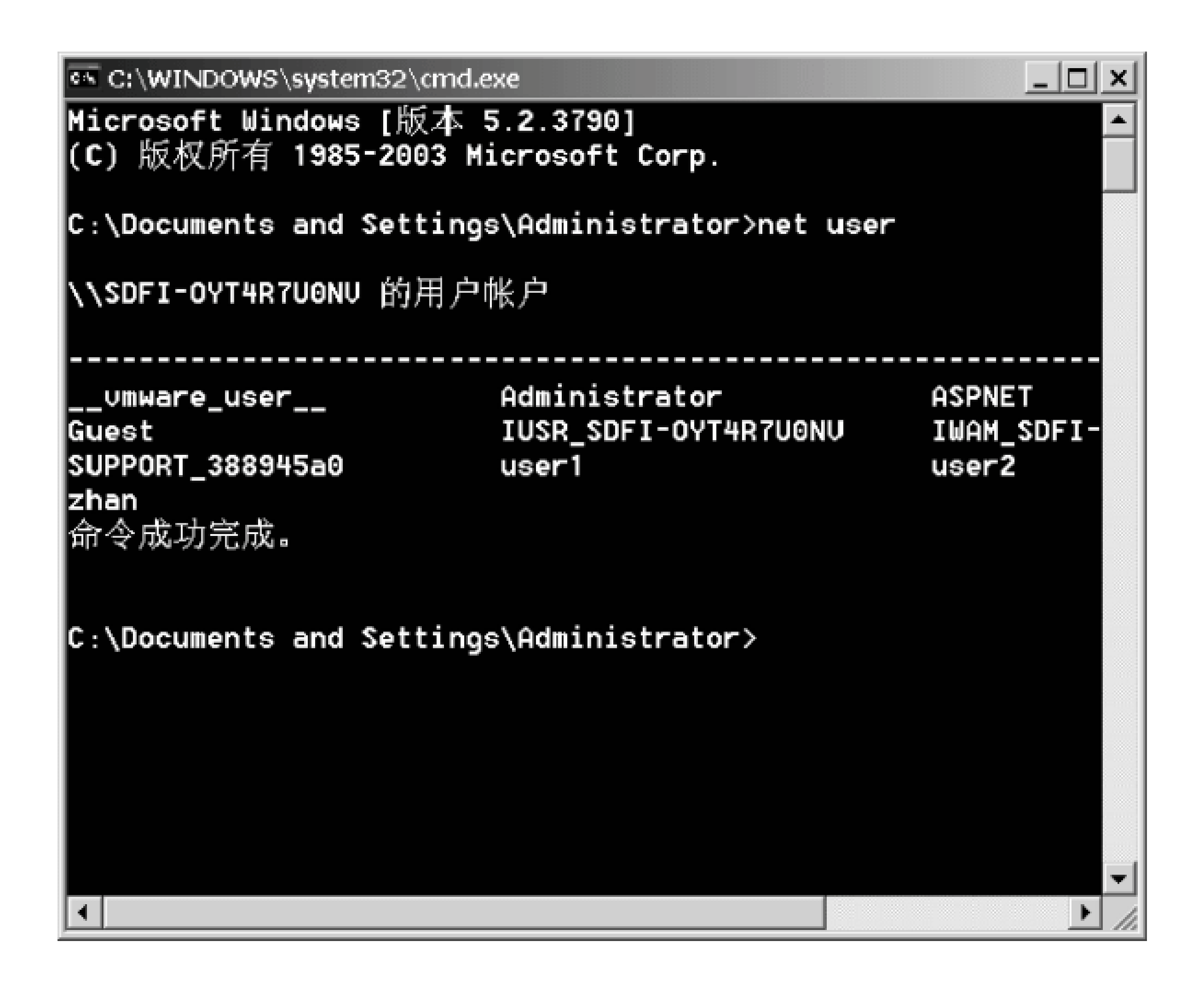


图 2.15　Net user 命令的使用



图 2.16　显示用户账号信息

Net view 命令的用法如下：

```
Net view [\computername | /domain[:domainname]]
         /network:nw [\computername]
```

当输入不带参数的 Net view 时，将显示当前域的计算机列表，如图 2.17 所示。

当输入\computername 参数时，则是指定要查看其共享资源的计算机。

（5）Net start 命令和 Net stop 命令

Net start 命令可用于启动或显示主机上的服务，当与远程主机建立连接并且取得 Shell 后，如果发现它的相关服务没有启动，就可以使用 Net start 命令来启动该服务。如果服务名是两个或两个以上的词，如 Http SSL 或 Event log，则必须用引号（"）引住。

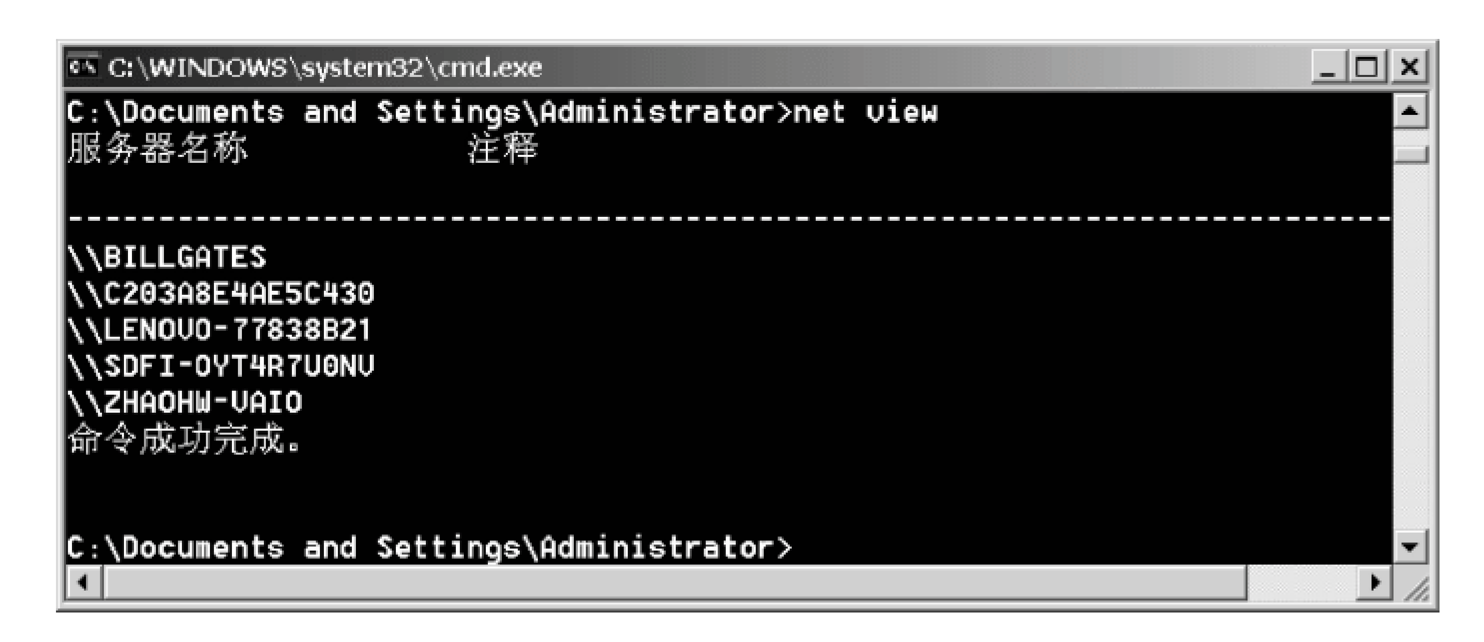


图 2.17 Net view 命令的使用

Net start 命令的用法如下：

```
Net start service
```

当输入不带参数的 Net start 命令时，则显示本地计算机上已开启的服务，如图 2.18 所示。



图 2.18 Net start 命令的使用

当输入 Net start alerter 时，则开启了服务 alerter，如图 2.18 所示。

Net stop 命令可用于停止主机上的服务。其用法如下：

```
Net stop service
```

当希望停止某个服务，如 alerter 服务时，可输入 net stop alerter 命令，如图 2.19 所示。

总之，灵活使用命令行环境下的上述命令能够便捷地检查和设置当前的网络状态。在网络状态的检查方面，不仅能够检查当前计算机的网络连接是否正常，以及网络连接的状态，而且能够查看局域网中存在哪些在线的计算机，以及通过何种路由到达这些计算机；在网络状态设置方面，我们能够设置登录计算机的账户，查看计算机的共享资源以及开启和关闭远程计算机的系统服务。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net start alerter
Alerter 服务正在启动 .
Alerter 服务已经启动成功。


C:\Documents and Settings\Administrator>net stop alerter

Alerter 服务已成功停止。


C:\Documents and Settings\Administrator>
```

图 2.19 开启 alerter 服务

2.6 实验思考

(1) 请思考，当 Ping 一台远程计算机时，若不成功，则可能在网络和计算机配置上存在哪些问题？

(2) 请通过实验检验 Administrator 账户能否被禁用。

实验3 计算机的安全配置

3.1 实验目的与要求

- 掌握如何删除不必要的系统服务以增强系统安全性。
- 掌握通过设置组策略来对计算机进行安全配置。
- 掌握通过修改注册表的方法来增强 Windows 2000 系统抗拒绝服务攻击的能力。
- 掌握如何阻止 ICMP 攻击。

3.2 实验环境

- 安装有 Windows 2000 系统的 PC 一台。
- 具有管理员权限的用户账户。

3.3 预备知识

1. Windows 的默认配置

Windows 操作系统预置了许多默认配置,以便于操作系统的使用以及计算机的互联和资源共享,然而,这些默认配置却存在着许多的安全隐患,容易带来信息安全问题。例如,在默认情况下,Windows 2000 系统启动后,通过 Net share 命令就可以在本地计算机上发现 admin $、IPC $、C $、D $ 等默认共享,这些默认共享有利于网络管理员便捷地管理远程的计算机设备,但是若这些计算机上的管理员账号被泄露,那么黑客就易于通过这些共享资源来获取非授权的信息。

因此,Windows 系统的默认配置仅是一种考虑了计算机系统普通应用情况的预置配置方式,当在自身的应用环境中使用安装有 Windows 操作系统的计算机时,应对其中的默认配置进行修改,以确保计算机系统的信息安全性。本实验将对默认配置中一些与安全有关的配置进行修改,用以提高计算机系统的安全性。

2. sc.exe

sc.exe 为一个用于与服务控制管理器和服务进行通信的命令行程

序。该程序主要有以下功能：

- 检索和设置有关服务的控制信息。
- 管理服务程序，如：测试、调试和删除服务程序。
- 设置存储在注册表中的服务属性来控制启动服务程序。

sc.exe 的用法如下：

```
sc <server> [command] [service name] <option1> <option2>...
```

其中，选项＜server＞的格式为\\ServerName，用于指定服务所在的远程服务器名称。参数[command]中包含 32 个命令，其中常用的命令有：

- query　查询服务的状态，或枚举服务类型的状态。
- start　启动服务。
- privs　更改服务的所需权限。
- qc　查询服务的配置信息。
- qdescription　查询服务的描述。
- delete　(从注册表)删除服务。
- create　创建服务(将其添加到注册表)。

3. 注册表的配置

注册表是 Windows 系统中的核心数据库，管理着系统运行所必需的重要数据。注册表中的数据来源于系统注册表文件和用户注册表文件两类，其中系统注册表文件包括：\system32\config 下的 Default、SAM、Security、Software、Userdiff 和 System 6 个文件；用户注册表文件包括\Documents and Setting\下的 ntuser.dat、ntuser.ini 和 ntuser.dat.log 3 个文件。通过 Windows 系统自带的 regedit.exe 注册表编辑器工具可以打开注册表数据库，对上述两类文件中的数据进行集中的配置和管理。而在本章的实验中，将演示如何通过修改注册表来加强 Windows 系统抗 DoS 攻击的能力。

4. ICMP 协议及攻击

ICMP(Internet Control Message Protocol)协议是 TCP/IP 协议族中众多协议中的一个，用于在主机之间、主机和路由器之间、路由器之间传递网络控制信息。这些控制信息不属于用户数据的一部分，但是对于整个网络的正常运行和维护却起着重要的作用，比如通过 ICMP 消息可以得知网络的连通性、主机是否在线、路由器是否可用等网络状态。

由于 ICMP 协议是一种网络控制协议，因此它是网络传输中的必要数据，也正因为此，它非常容易被用来攻击网络中的主机和路由器。例如，大量的 ICMP 数据包会形成 ICMP 风暴，当主机受到这种 ICMP 数据风暴的攻击时，其处理器会耗费大量的资源来处理这些 ICMP 数据，这最终会导致整个主机系统的瘫痪。

3.4 实验内容

本章的实验内容主要包括以下 4 部分

(1) 演示如何使用命令行中的命令卸载和删除 tlntsvr 服务。

(2) 演示如何隐藏驱动器、禁止来宾账户、开启审核策略和 IE 浏览器的安全设置，以加强系统的安全性。

(3) 演示如何通过对注册表的修改来防范 DoS 攻击。

(4) 演示如何通过添加过滤规则来过滤 ICMP 报文，从而彻底杜绝这种攻击。

3.5　实验步骤

3.5.1　卸载和删除 tlntsvr 服务

首先在桌面上右击“我的电脑”，在弹出的快捷菜单中选择“管理”，打开“计算机管理”窗口。在该对话框左边的列表中展开“服务和应用程序”，并单击下属的“服务”列表项，这样在“计算机管理”窗口的右边则会出现本地计算机所支持的各种服务，如图 3.1 所示。



图 3.1　“计算机管理”窗口

双击其中的 Telnet 列表项，则可对该服务进行启动、停止、暂停和恢复操作，如图 3.2 所示。但是，Windows 操作系统并没有提供一个图形界面来对其实施卸载和删除操作。

下面通过 sc.exe 命令来演示如何卸载 Telnet 服务(即 TlntSvr 服务)。

单击“开始”→“运行”命令，在弹出的“运行”对话框中输入 CMD 命令，单击“确定”按钮，从而打开命令行窗口。

在命令行窗口中可以输入 sc qc tlntsvr，查看 tlntsvr 服务的配置信息，如图 3.3 所示。可以看到 tlntsvr 服务所对应的二进制程序为：

```
c:\windows\system32\tlntsvr.exe.
```



图 3.2 Telnet 服务的状态



图 3.3 tlntsvr 服务配置信息

为了将 tlntsvr 服务卸载，先在命令行窗口中通过命令 sc stop tlntsvr 停止该服务，然后通过命令 sc delete tlntsvr 将 tlntsvr 服务在服务列表中删除，如图 3.4 所示。

单击“计算机管理”对话框中工具栏的“刷新”按钮后，会发现在右边的服务列表中已没有了 Telnet 服务(即 tlntsvr 服务)，如图 3.5 所示。

利用类似方法可以禁止和删除其他一些想要删除的服务。例如，Schedule 服务非常容易被黑客利用来执行一些系统命令和可执行文件，如果仅是简单地停止 Schedule 服务，也不能保证安全性，因为有些黑客工具可以远程地开启该服务。

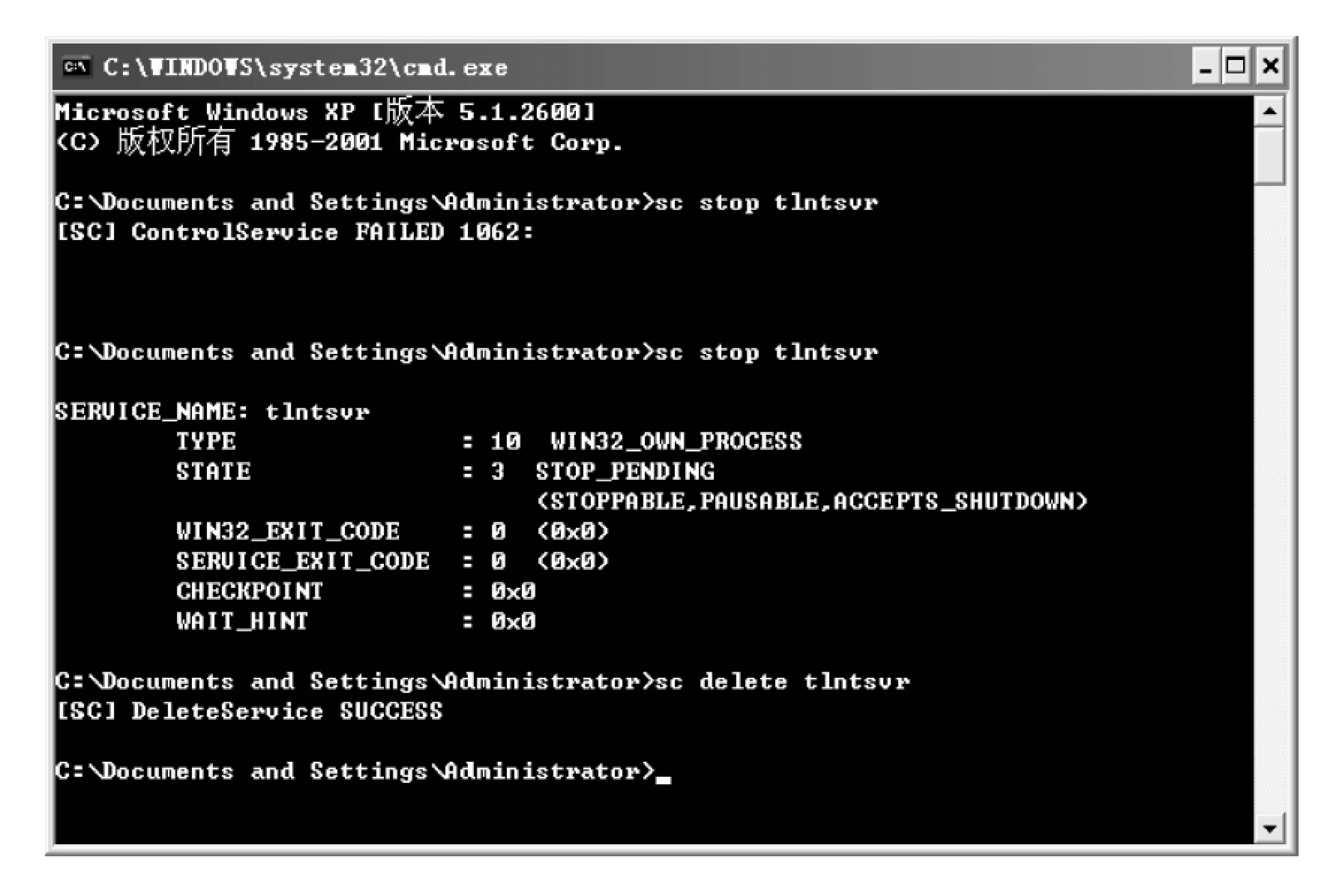


图 3.4　停止并删除 tlntsvr 服务



图 3.5　删除 tlntsvr 服务后的效果

3.5.2　使用 Windows 组策略对计算机进行安全配置

单击“开始”→“运行”命令，在弹出的“运行”对话框中输入 gpedit.msc，单击“确定”按钮，即可打开“组策略”窗口，如图 3.6 所示。下面的四种安全配置将在“组策略”窗口中完成。



图 3.6 "组策略"窗口

1. 隐藏驱动器

选择"用户配置"→"管理模板"→"Windows 组件"→"Windows 资源管理器"→"隐藏'我的电脑'中的这些指定的驱动器",打开相应的对话框,如图 3.7 所示,在对话框中选择"已启用"选项,并在其下的下拉列表框中选择一个组合,单击"确定"按钮后,组合框中选中的驱动器符号就不会出现在标准的打开对话框中。



图 3.7 隐藏驱动器名称

但需要注意的是，这项策略仅删除驱动器的图标，用户仍然可以通过其他方式访问驱动器的内容，如：通过在映射网络驱动器对话框、运行对话框或命令窗口上输入一个驱动器的目录路径。同时，此策略不会防止用户使用程序访问这些驱动器或其内容，也不会防止用户使用“磁盘管理”管理单元查看并更改驱动器特性。

2. 禁止来宾账户本机登录

当人们暂时离开工作电脑时，可能有一些打开的文档还在处理之中，为了避免其他人动用电脑，一般会将电脑锁定。但是，当电脑处于局域网环境下时，可能已在本地电脑上创建了一些来宾账户，以方便他人的网络登录需求。但是其他人也可以利用这些来宾账号注销当前账号并进行本地登录，这样会对当前的文档处理工作造成影响。为了解决该问题，可以通过“组策略”的设置来禁止一些来宾账号的本地登录，仅保留它们的网络登录权限。

在“组策略”窗口的左侧依次选择“计算机配置”→“Windows 配置”→“安全配置”→“本地策略”→“用户权利指派”，然后在“组策略”窗口的右侧双击“拒绝本地登录”，则弹出“拒绝本地登录 属性”对话框，如图 3.8 所示。



图 3.8 “拒绝本地登录 属性”对话框

在该对话框中通过单击“添加用户或组”按钮，则弹出“选择用户或组”对话框，如图 3.9 所示，然后单击左下方的“高级”按钮，在弹出的对话框中单击左侧的“立即查找”按钮，则会在对话框下方显示出本计算机上的所有账户，如图 3.10 所示，选中所需的账户 temp，单击“确定”按钮，则将 temp 用户加入到禁止登录的账户列表中，如图 3.11 所示。



图 3.9 “选择用户或组”对话框

3. 开启审核策略

在“组策略”对话框的左侧依次选择“计算机配置”→“Windows 配置”→“安全配置”→“本地策略”→“策略审核”，然后在“组策略”窗口的右侧就会出现各种审核策略的设置项，其

中包括审核策略更改、登录事件、对象访问、过程追踪、目录服务访问、特权使用等，如图 3.12 所示。

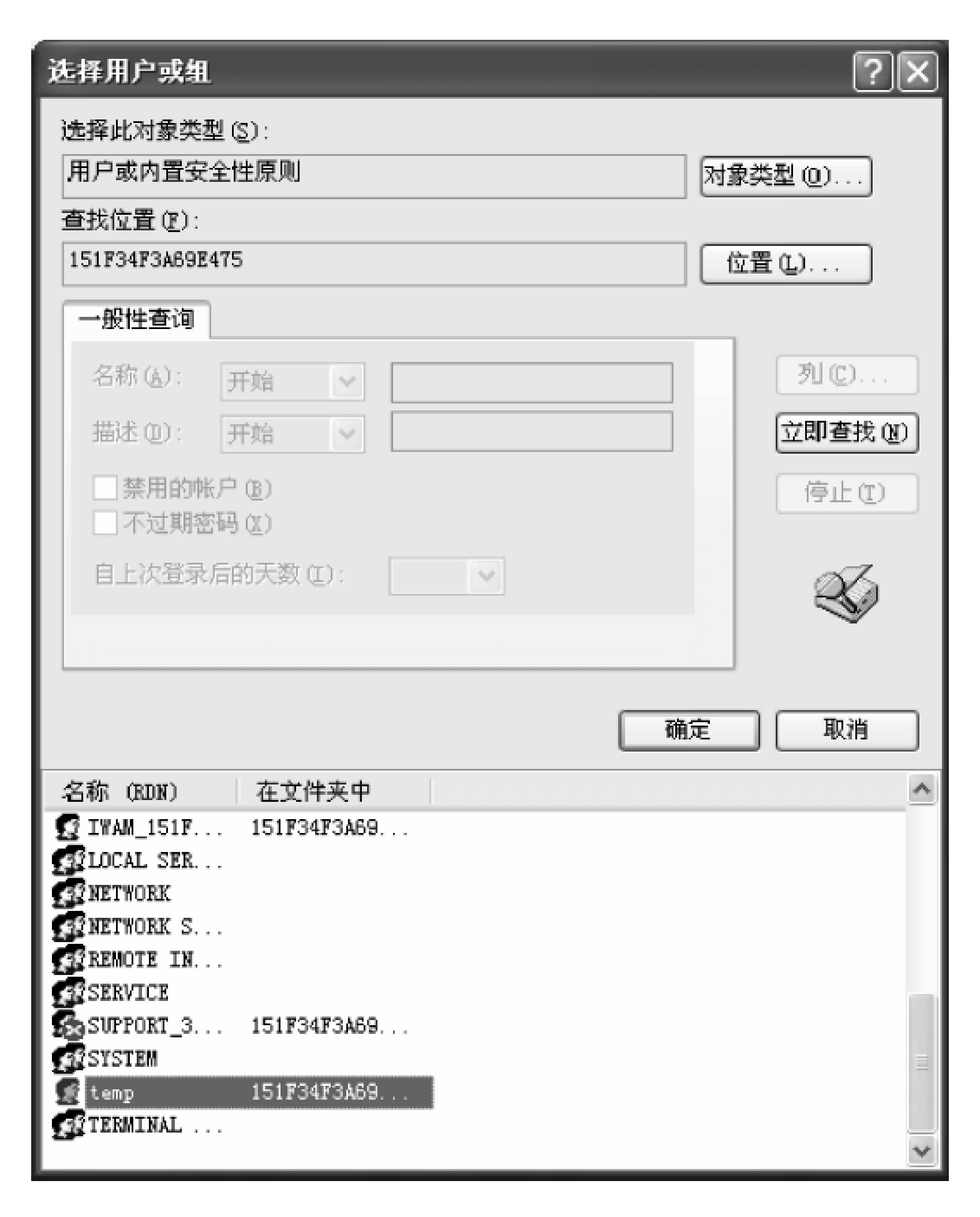


图 3.10 查找需要禁止登录的账户



图 3.11 将指定账号添加到禁止登录列表中



图 3.12 查看审核策略

通过设置各个审核策略，系统便可记录相应的事件。比如，双击“审核登录事件”后，在弹出的“审核登录事件 属性”对话框中选中“成功”和“失败”两个选项，如图 3.13 所示，则系统将会自动记录用户何时登录过系统。

值得注意的是，系统管理员应养成时常查看“控制面板”→“管理工具”→“事件查看器”中所记录的事件的习惯。比如，若“组策略”被修改后系统发生了问题，“事件查看器”就会及时显示修改了哪些策略；在“登录事件”里，系统管理员可以查看详细的登录事件，知道谁曾尝试使用禁用的账户登录、谁的账户密码已过期等。



图 3.13 审核登录事件的设置

4. IE 浏览器的安全设置

在“组策略”窗口的左侧依次选择“用户配置”→“管理模板”→“Windows 组件”→Internet Explorer 分支，在右侧窗口中会出现“Internet 控制面板”、“浏览器菜单”、“工具栏”、“持续行为”和“管理员认可的控件”等策略选项，利用它可以充分打造一个极有个性和安全的 IE 浏览器。

(1) 禁止修改 IE 浏览器主页

当用户上网时，一些恶意网站通过自身的恶意代码会对用户的 IE 浏览器主页的设置进行修改，从而对用户的上网行为造成影响。为了避免此类事件的发生，可以在“组策略”窗口的左侧依次选择“用户配置”→“管理模板”→“Windows 组件”→Internet Explorer，如图 3.14 所示。

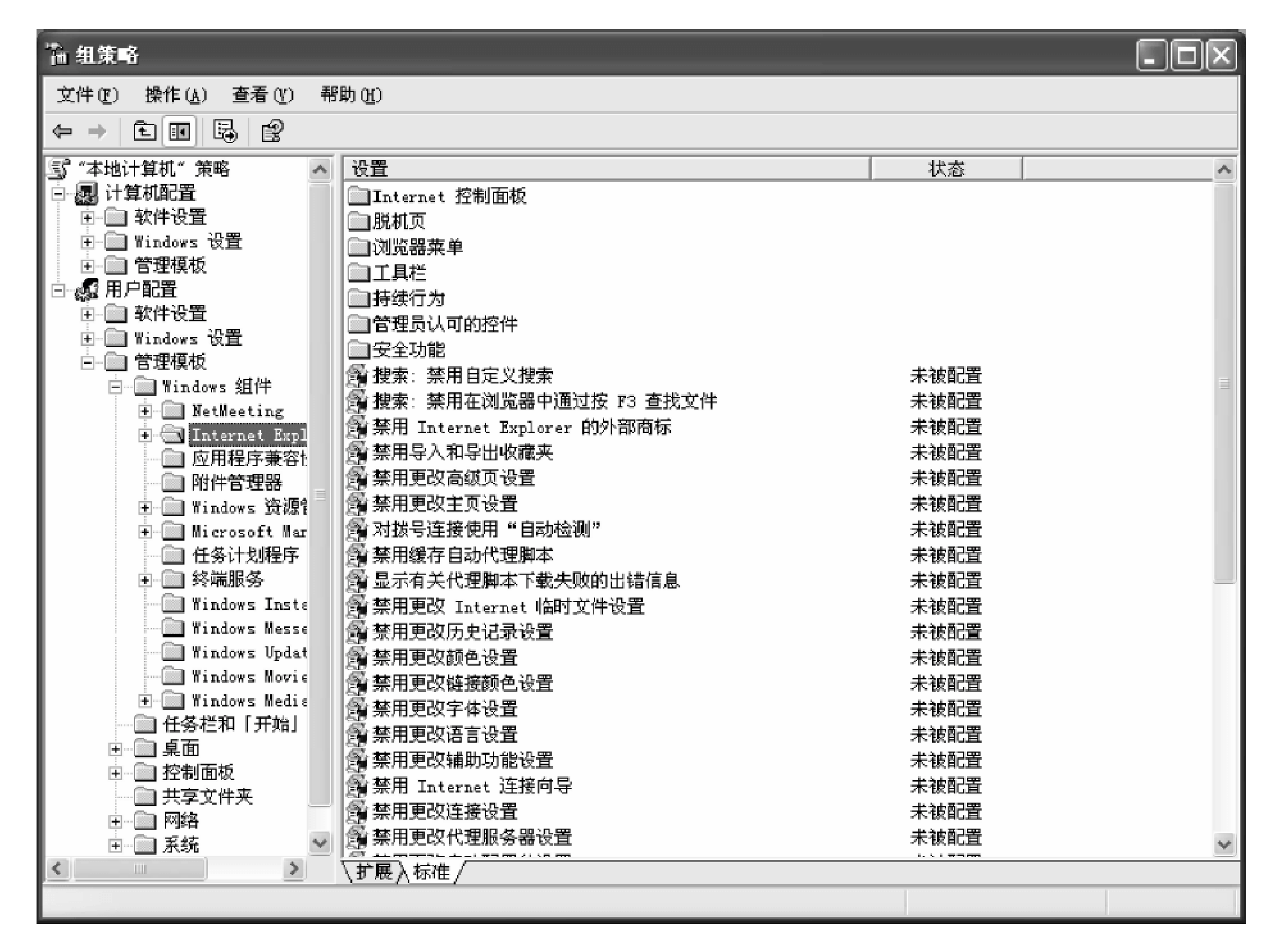


图 3.14 IE 的安全设置

然后在右侧的窗口中双击“禁用更改主页设置”策略，在弹出的对话框中选中“已启用”单选按钮，并单击“确定”按钮即可，如图3.15所示。

(2) 禁用“常规”选项卡

如图3.14所示，在加固IE的安全选项中还提供了“禁止更改历史记录设置”、“禁止更改颜色设置”以及“禁止更改Internet临时文件设置”等策略。如果启用了这些安全策略，在IE浏览器的“Internet选项”对话框中“常规”选项卡的“主页”区域的设置将变灰。但如果在“用户配置”→“管理模板”→“Windows组件”→Internet Explorer→“Internet控制面板”中双击“禁用常规页”策略，并在弹出的“禁用常规页 属性”对话框中选中“已禁用”，如图3.16所示，则无需设置该策略，因为“禁用常规页”策略将删除界面上的“常规”选项卡。



图3.15 禁止更改IE主页设置



图3.16 禁用IE浏览器中的常规页

(3) IE安全的高级配置

在图3.14的右侧部分，可以看到还列出了7个子文件夹，单击其中的每一个子文件夹，均可显示出一组关于IE安全的配置项。其中“Internet控制面板”包含了一组从“Internet选项”对话框“添加”和“删除”选项卡的设置；“脱机页”包含了脱机页和频道的设置；“浏览器菜单”包含了显示和隐藏Internet Explore中菜单和菜单选项的设置；“工具栏”包含允许和限制用户编辑Internet Explore的工具栏；“持续行为”包含了Internet安全区域的文件大小限制的设置；“管理员认可的控件”包含了启用和禁止ActiveX控件的设置；“安全功能”包含了启用和禁用Internet Explorer、Windows Explorer和其他应用程序的安全功能的设置。对这些设置选项进行适当的配置，会大大增强IE的安全性。

3.5.3 加固Windows抗DoS攻击能力

下面通过修改注册表的方法来提高Windows 2000系统抵抗DoS攻击(Deny of Services，拒绝服务攻击)的能力。所采用的方法是：单击“开始”→“运行”命令，在“运行”对话框中输入regedit.exe，单击“确定”按钮，打开注册表编辑器。然后在相应的位置下右键

单击需要修改的项，在弹出的快捷菜单中选择“修改二进位数据”，进行相应的修改。如图 3.17 所示。



图 3.17　修改注册表

1. 在[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\Tcpip\Parameters]位置下对以下键值作修改。

(1) 关闭无效网关的检查。当服务器设置了多个网关，这样在网络不通畅的时候系统会尝试连接第二个网关，通过关闭它可以优化网络。

修改项：“EnableDeadGWDetect”=dword：00000000

(2) 禁止相应 ICMP 重定向报文。此类报文有可能用于攻击，所以系统应该拒绝接受 ICMP 重定向报文。

修改项：“EnableICMPRedirects”=dword：00000000

(3) 不允许释放 NETBIOS 名。当攻击者发出查询服务器 NETBIOS 名的请求时，可以使服务器禁止响应。注意系统必须安装 SP2 以上。

修改项：“NoNameReleaseOnDemand”= dword：00000001

(4) 发送验证保持活动数据包。该选项决定 TCP 间隔多少时间来确定当前连接还处于连接状态。若不设该值，则系统每隔 2 小时对 TCP 是否有闲置连接进行检查，这里设置时间为 5 分钟。

修改项：“KeepAliveTime”= dword：000493e0

(5) 禁止进行最大包长度路径检测。该项值为 1 时，将自动检测出可以传输的数据包的大小，可以用来提高传输效率，如出现故障或者安全起见，设项值为 0，表示使用固定的 MTU 值 576bytes。

修改项：“EnablePMTUDiscovery”= dword：00000000

(6) 启动 SYN 攻击保护。默认项值为 0，表示不开启攻击保护；项值为 1 和 2 表示启

动 syn 攻击保护，设为 2 之后安全级别更高，对何种状况下认为是攻击，则需要根据下面的 TcpMaxHalfOpen 和 TcpMaxHalfOpenRetried 值设定的条件来触发启动。这里需要注意的是，NT4.0 必须设为 1，设为 2 后在某种特殊数据包下会导致系统重启。

修改项："SynAttackProtect"= dword：00000002

(7) 同时允许打开的半连接数量。所谓半连接，表示未完整连接的 TCP 会话，用 netstat 命令可以看到呈 SYN_RCVD 状态的就是。这里使用微软的建议值，服务器设为 100，高级服务器设为 500。建议可以设稍微小一点。

修改项："TcpMaxHalfOpen"= dword：00000064

(8) 判断是否存在攻击的出发点。这里使用微软的建议值，服务器为 80，高级服务器为 400。

修改项："TcpMaxHalfOpenRetried"= dword：00000050

(9) 设置等待 SYN_ACK 时间。默认项值为 3，默认这一过程消耗时间 45 秒；项值为 2，消耗时间为 21 秒；项值为 1，消耗时间为 9 秒。最低可以设为 0，表示不等待，消耗时间为 3 秒。这个值可以根据遭受攻击规模修改。微软站点安全推荐为 2。

修改项："TcpMaxConnectResponseRetransmissins"= dword：00000001

(10) 设置 TCP 重传单个数据段的次数。默认项值为 5，默认这一过程消耗时间为 240 秒。微软站点安全推荐为 3。

修改项："TcpMaxDataRetransmissins"= dword：00000003

(11) 设置 syn 攻击保护的临界点。当可用的 backlog 变为 0 时，此参数用控制 syn 攻击保护的开启，微软站点安全腿脚为 5。

修改项："TCPMaxPortsExhausted"= dword：00000005

(12) 禁止 IP 源路由。默认项值为 1，表示不转发源路由包；项值设为 0，表示全部转发；项值设为 2，表示丢弃所有接收的源路由包。微软站点安全推荐为 2。

修改项："DisableIPSourceRouting"= dword：00000002

(13) 限制处于 TIME_WAIT 的最长时间。默认为 240 秒，最低为 30 秒，最高为 300 秒。建议设为 30 秒。

修改项："TcpTimedWaitDelay"= dword：0000001e

2. 在[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]位置下对以下键值作修改。

(1) 调整 NetBT 的连接块增加幅度。默认为 3，范围 1～20，数值越大，在连接越多时可提升性能。每个连接块消耗 87 字节。

修改项："BacklogIncrement"= dword：00000003

(2) 最大 NetBT 的连接块的数目。范围 1～40 000，这里设置为 1000，数值越大，在连接越多时允许更多连接。

修改项："MaxConnBacklog"= dword：00000003

3. 在[HKEY_LOCAL_M：CHINE\SYSTEM\CurrentControlSet\Services\Afd\Parameters]位置下对以下键值作修改。

(1) 配置激活动态 Backlog。对于网络繁忙或者容易遭受 SYN 攻击的系统，建议设置为 1，表示允许动态 Backlog。

修改项："EnableDynamicBacklog"= dword：00000001

(2) 配置最小动态 Backlog。默认项值是 0，表示动态 Backlog 分配的自由连接的最小数目。当自由连接数目低于此数目时，将自动的分配自由连接。对于网络繁忙或者易遭受 SYN 攻击的系统，建议设置为 20。

修改项："MinimumDynamicBacklog"= dword：00000014

(3) 最大动态 Backlog。表示定义最大"准"连接的数目，主要看内存大小，理论每 32M 内存最大可以增加 5000 个，这里设为 20 000。

修改项："MaximumDynamicBacklog"= dword：00002e20

(4) 每次增加的自由连接的数量。默认项值为 5，表示定义每次增加的自由连接数目。对于网络繁忙或者易遭受 SYN 攻击的系统，建议设置为 10。

修改项："DynamicBacklogGrowthDelta"= dword：0000000a

4. 根据需要对以下键值作修改：

(1) 启用网卡上的安全过滤

在[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]位置下修改项："EnableSecurityFilters"= dword：00000001

(2) 禁止路由发现功能

在[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{自己的网卡接口}]位置下修改项："PerformRouterDiscovery"= dword：00000000

3.5.4 通过过滤 ICMP 报文阻止 ICMP 攻击

很多针对 Windows 2000 系统的攻击均是通过 ICMP 报文的漏洞攻击实现的，如 Ping of Death 攻击。下面我们通过安全配置来过滤 ICMP 报文，从而阻止 ICMP 攻击。

1. 启动"本地安全设置"

在"控制面板"中打开"管理工具"，从中双击"本地安全策略"，从而打开"本地安全设置"窗口，如图 3.18 所示。

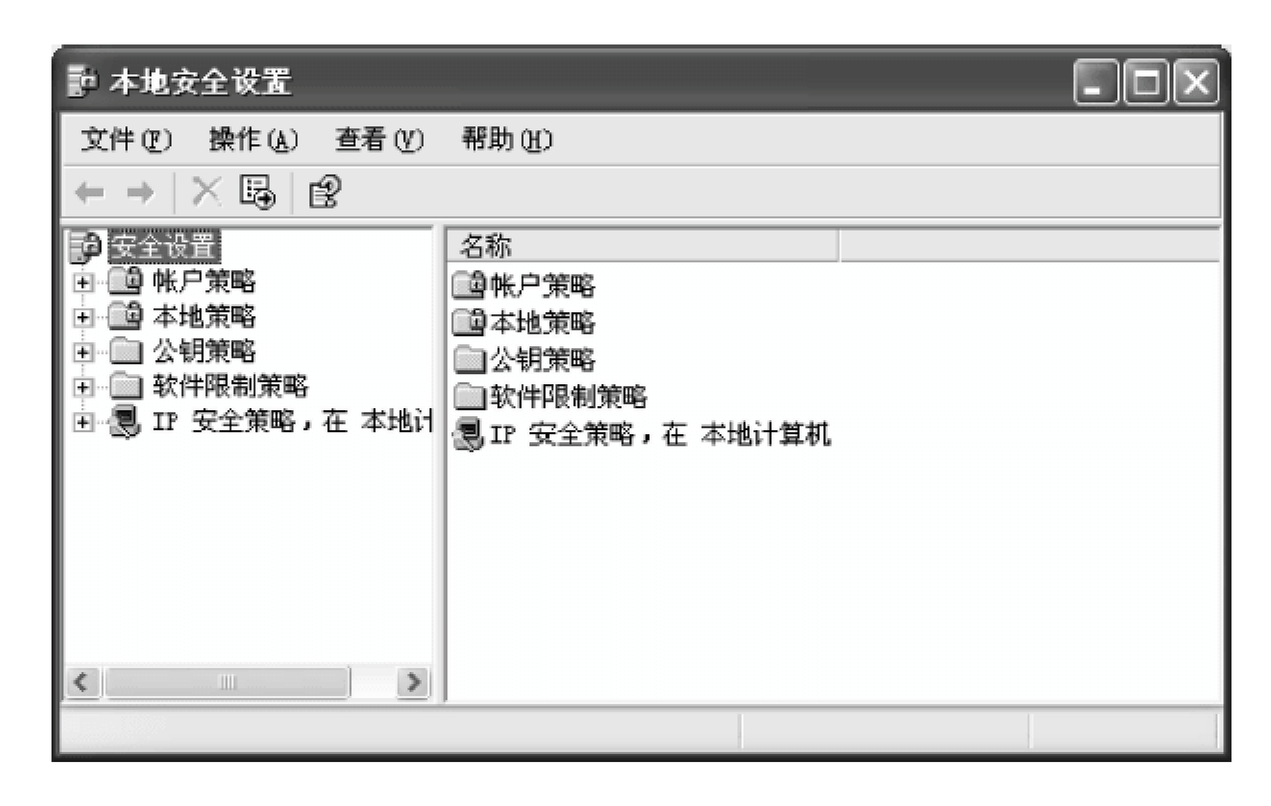


图 3.18 "本地安全设置"窗口

2. ICMP 过滤规则的添加

在"本地安全设置"窗口中，右键单击"IP 安全策略，在本地计算机"并从弹出的快捷菜单中选择"管理 IP 筛选器和 IP 筛选器操作"，从而弹出"管理 IP 筛选器和筛选器操作"对话框。在该对话框的"管理 IP 筛选器列表"属性页中，单击左下方的"添加"按钮，弹出"IP 筛选器列表"对话框。在该对话框的"名称"框中输入"防止 ICMP 攻击"，并取消选中右侧的"使用'添加向导'"复选框，如图 3.19 所示。

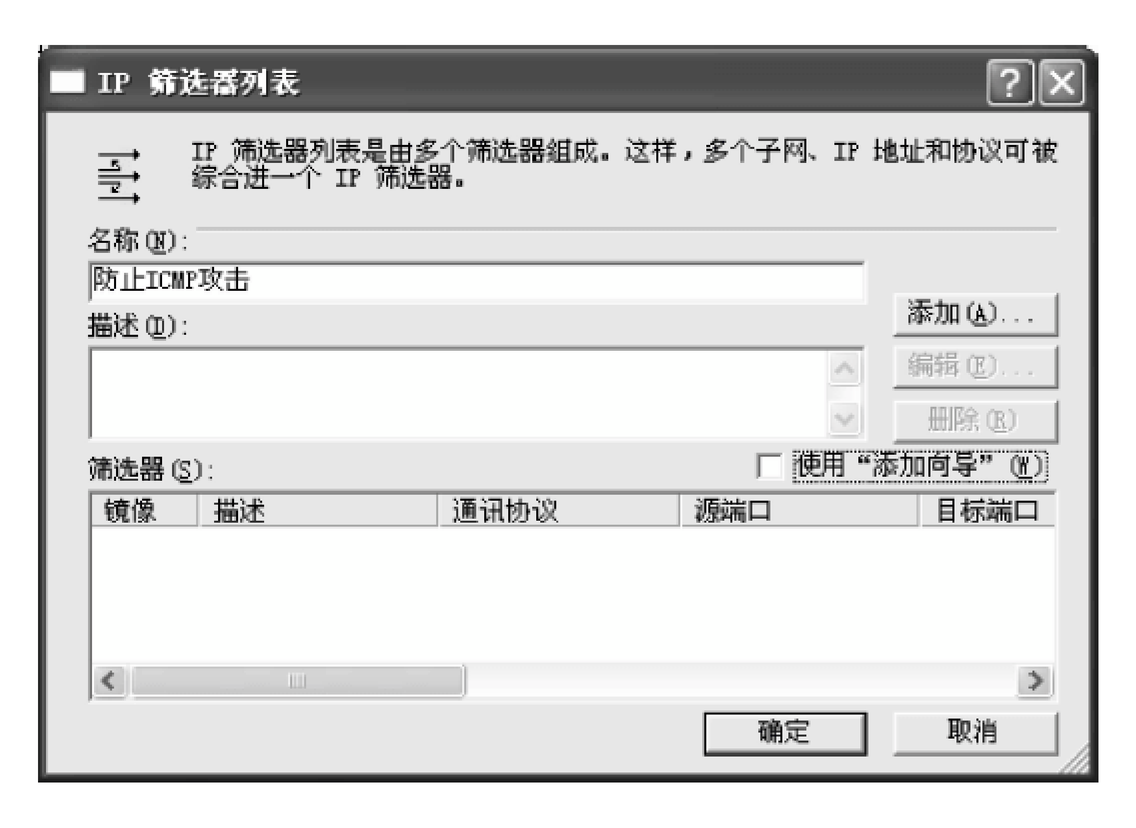


图 3.19 IP 筛选器列表

单击图 3.19 右侧的"添加"按钮，弹出"筛选器 属性"对话框。在该对话框的"寻址"属性页中，源地址选择"任何 IP 地址"，目标地址选择"我的 IP 地址"，如图 3.20 所示；在"协议"属性页中，协议选择 ICMP，然后单击"确定"按钮，设置完毕。

在"管理 IP 筛选器和筛选器操作"对话框中选择"管理筛选器操作"属性页，取消选中右下方的"使用'添加向导'"复选框，然后单击左下方的"添加"按钮，弹出"新筛选器操作 属性"对话框，如图 3.21 所示。



图 3.20 "筛选器 属性"对话框

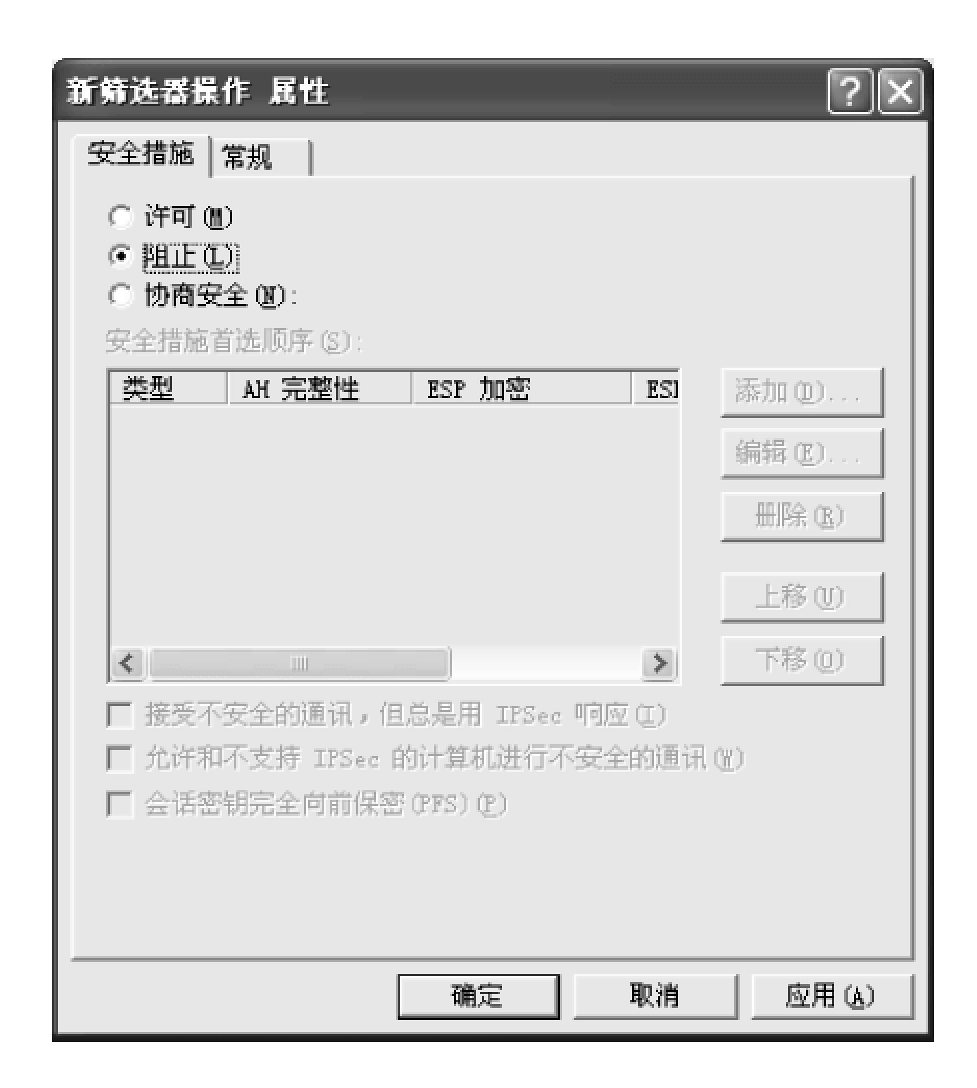


图 3.21 "新筛选器操作 属性"对话框

在该对话框的“安全措施”属性页中选择“阻止”，在“常规”属性页中输入“Deny 操作”，单击“确定”按钮。

这样，就设置了一个关注所有进入 ICMP 报文的过滤策略和丢弃所有报文的过滤操作了。

3. 添加 ICMP 过滤器

① 在“本地安全设置”对话框中，右键单击“IP 安全策略 在本地计算机”，在弹出的快捷菜单中选择“创建 IP 安全策略”，则弹出“IP 安全策略向导”对话框，单击“下一步”按钮，在“IP 安全策略名称”处输入“ICMP 过滤器”，如图 3.22 所示。

② 依次单击“下一步”按钮，完成“IP 安全策略向导”的设置。然后在“ICMP 过滤器”对话框的“规则”属性页中，取消“使用‘添加向导’”，并单击左下方的“添加”按钮，弹出“新规则属性”对话框。在该对话框的“IP 筛选器列表”属性页中，选中“防止 ICMP 攻击”，如图 3.23 所示。在“筛选器操作”属性页中选择“Deny 操作”，然后单击“确定”按钮，设置完毕。



图 3.22 “IP 安全策略向导”对话框

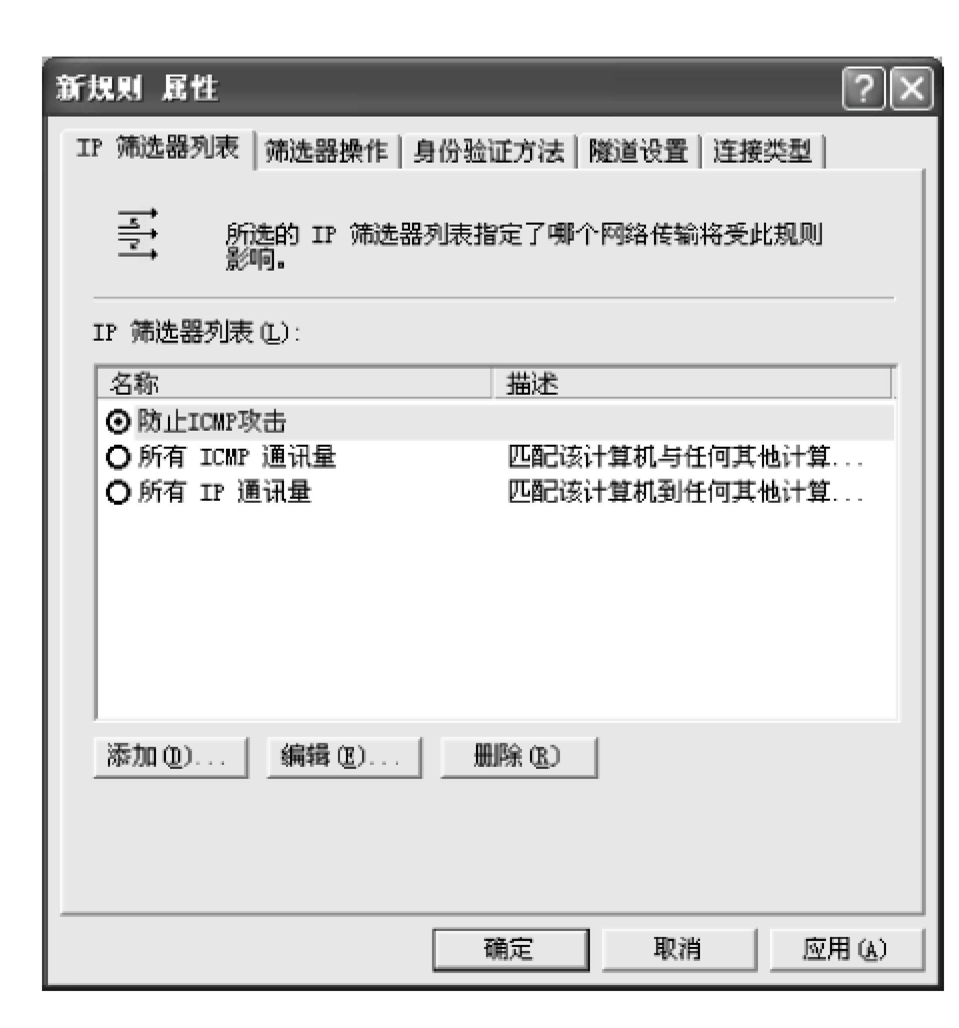


图 3.23 IP 筛选器列表

③ 在“本地安全设置”窗口中，选择窗口左侧的“IP 安全策略，在本地计算机”，然后在窗口右侧右键单击“ICMP”过滤器，在弹出的快捷菜单中选择“指派”，如图 3.24 所示。

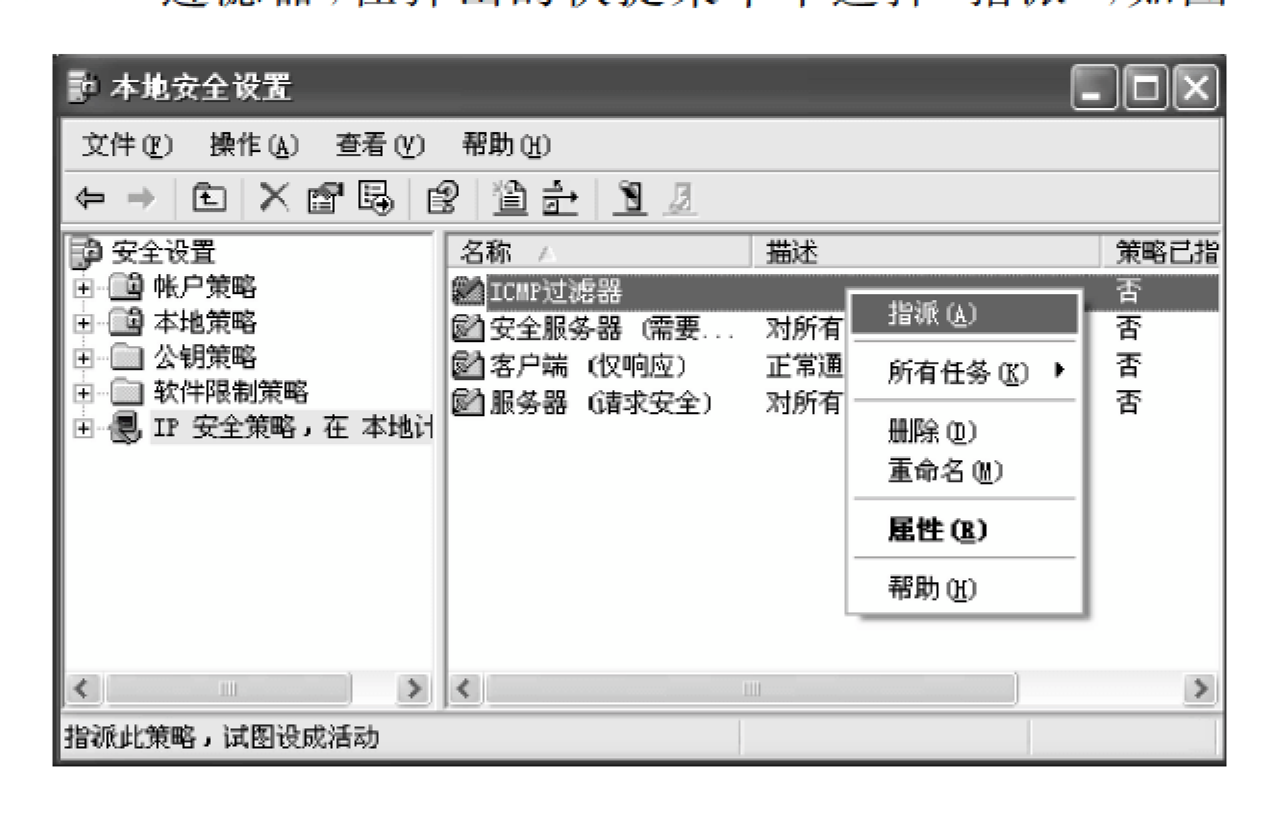


图 3.24 指派 ICMP 过滤操作

这样，就完成了一个关注所有进入系统的 ICMP 报文的过滤策略和丢弃所有报文的过滤操作，从而阻挡攻击者使用 ICMP 报文进行的攻击。

上述实验内容分别展示了如何在 Windows 系统中删除和卸载系统服务，利用组策略对系统进行安全加固，如何应对 DoS 攻击以及如何设置过滤策略阻止 ICMP 报文的攻击。综合利用上述手段对系统进行灵活配置，将能打造出一个相对安全的 Windows 系统环境。

3.6 实验思考

(1) 思考是不是所有的系统服务都能关闭和删除，为什么？

(2) 请思考如何关闭系统的 U 盘“自动播放”功能？即在计算机上插入 U 盘后，禁止系统自动播放 U 盘中的文件。

第2篇

安全配置篇

ARTICLE 2

实验4　NTFS 文件系统实验

4.1　实验目的与要求

• 了解 NTFS 文件系统的特点。

• 掌握查看 NTFS 版本号以及将 FAT 文件系统转化为 NTFS 文件系统的方法。

• 掌握 NTFS 中权限的含义和文件权限的设置方法。

4.2　实验环境

Windows XP 操作系统。

4.3　预备知识

新技术文件系统（New Technology File System，NTFS）是 Microsoft 公司为了弥补 FAT 文件系统的一些不足而推出的一项新的磁盘文件管理技术，其最大的特点是具有良好的稳定性、容错性和安全性。它是 Windows 2000 Server 推荐使用的高性能文件系统，目前已在 Windows XP 系列、Windows Server 2003 系列、Windows Server 2008 系列以及 Windows Vista 等操作系统上得到了广泛的应用，并发挥出巨大的文件管理作用。目前常用的 NTFS 版本号为 3.1，已经推出 NTFS 5.0 与 NTFS-3G 版本，其中 NTFS-3G 可用于 Linux 操作系统。

NTFS 系统与 FAT 系统相比，有诸多优点，NTFS 通过使用标准的事务处理记录和还原技术来保持卷的一致性，如果系统出现故障，NTFS 将使用日志文件和检查点信息来恢复文件系统的一致性。此外，NTFS 还可以提供文件和文件夹权限、加密、磁盘配额和压缩等高级功能。

1. 文件和文件夹权限

NTFS 分区中，对于每一个文件以及文件夹，NTFS 都存有相应的访问控制列表（Access Control List，ACL），其中包含所有被许可的用户账户、组和计算机。ACL 中包含访问控制项（Access Control Entity，ACE），若在文件或文件夹的访问控制列表中没有相应的 ACE，则对文件

的访问会被拒绝。

NTFS 权限可用来指定哪个用户、用户组和计算机可对文件和文件夹进行何种访问。例如，NTFS 支持对文件进行下列权限的操作：

- 读　可以读取文件，查看文件的属性、所有者以及权限。
- 写　可以写入数据、覆盖文件、修改文件属性，以及查看文件权限和所有权。
- 读和运行　可以读取文件，查看文件的属性、所有者、权限，还可以运行应用程序。
- 修改　可以读取并写入/修改文件，查看并更改文件的属性、所有者、权限，还可以运行应用程序以及删除文件。
- 完全控制　对文件的最高权力，在拥有上述其他权限所有的权限以外，还可以修改文件权限以及替换文件所有者。

对于文件夹，NTFS 支持以下权限的操作：

- 读　读取文件和查看子文件夹，查看文件夹属性、所有者和权限。
- 写　创建文件夹、修改文件夹属性、查看文件夹权限和所有者。
- 列出文件夹内容　查看此文件夹中的文件和子文件夹。
- 读和运行　遍历文件夹，查看并读取文件和查看子文件夹，查看文件夹属性、所有者和权限。
- 修改　除了查看并读取文件和查看子文件夹、创建文件和子文件夹、查看和修改文件夹属性、所有者和权限以外，还可以删除文件夹。
- 完全控制　文件夹的最高权限，在拥有上述所有文件夹权限外，还可以修改文件夹权限、替换所有者以及删除子文件夹。

除此之外，NTFS 还有一些特殊权限。

2. 加密

NTFS 的数据加密特性称作加密文件系统(EFS，Encrypting File System)，可以用 EFS 加密 NTFS 分区中的数据。Windows 2000、XP 专业版以及 Windows Server 2003 都支持 EFS，但是，Windows XP 家庭版不支持。EFS 是一个透明的文件加密服务，它以公钥基础设施(PKI，Public Key Infrastructure)为平台，使用 CryptoAPI 架构。EFS 提供可选的数据恢复能力，系统管理员可以恢复另一用户加密的数据。EFS 也可以实现多用户(被许可的用户)共享存取一个已经加密的文件夹。

3. 磁盘配额

在 Windows 2000/XP 系统中，NTFS 支持磁盘配额，以控制用户在服务器中的磁盘用量，当用户使用了一定的服务器磁盘空间以后，系统可以：①发出警告；②禁止用户对服务器磁盘的使用；③将事件记录到系统日志中。这样，域中的用户便不可随意使用服务器磁盘空间，在服务器磁盘中存放过期的、杂乱的个人文件了。当然，磁盘配额在个人计算机中也可使用，并可使磁盘管理更加方便。

4. 压缩

NTFS 文件系统提供了数据压缩的功能，我们可以压缩不常使用的数据从而节省磁盘

空间。这种压缩对于用户是透明的，当我们访问一个使用 NTFS 压缩的文件夹时，并看不到解压缩的过程。然而，每当我们对压缩文件或文件夹进行访问时，系统在后台自动解压缩数据；当我们访问结束后，系统再自动压缩数据。

4.4 实验内容

本章实验包括 3 部分的内容：

(1) 演示如何查看 Windows 系统的 NTFS 版本号。

(2) 演示如何通过命令行方式和界面方式将 FAT 系统转化为 NTFS 系统。

(3) 演示如何对 NTFS 系统下的文件夹实施授权控制管理。

4.5 实验步骤

4.5.1 查看 NTFS 的版本号

① 单击“开始”→“运行”命令。

② 在弹出的“运行”对话框中输入 cmd 命令，然后单击对话框下方的“确定”按钮。如图 4.1 所示。

③ 在弹出的 cmd.exe 窗口中输入：“fsutil fsinfo ntfsinfo C:”，按下 Enter 键，显示如图 4.2 所示画面。



图 4.1 “运行”对话框

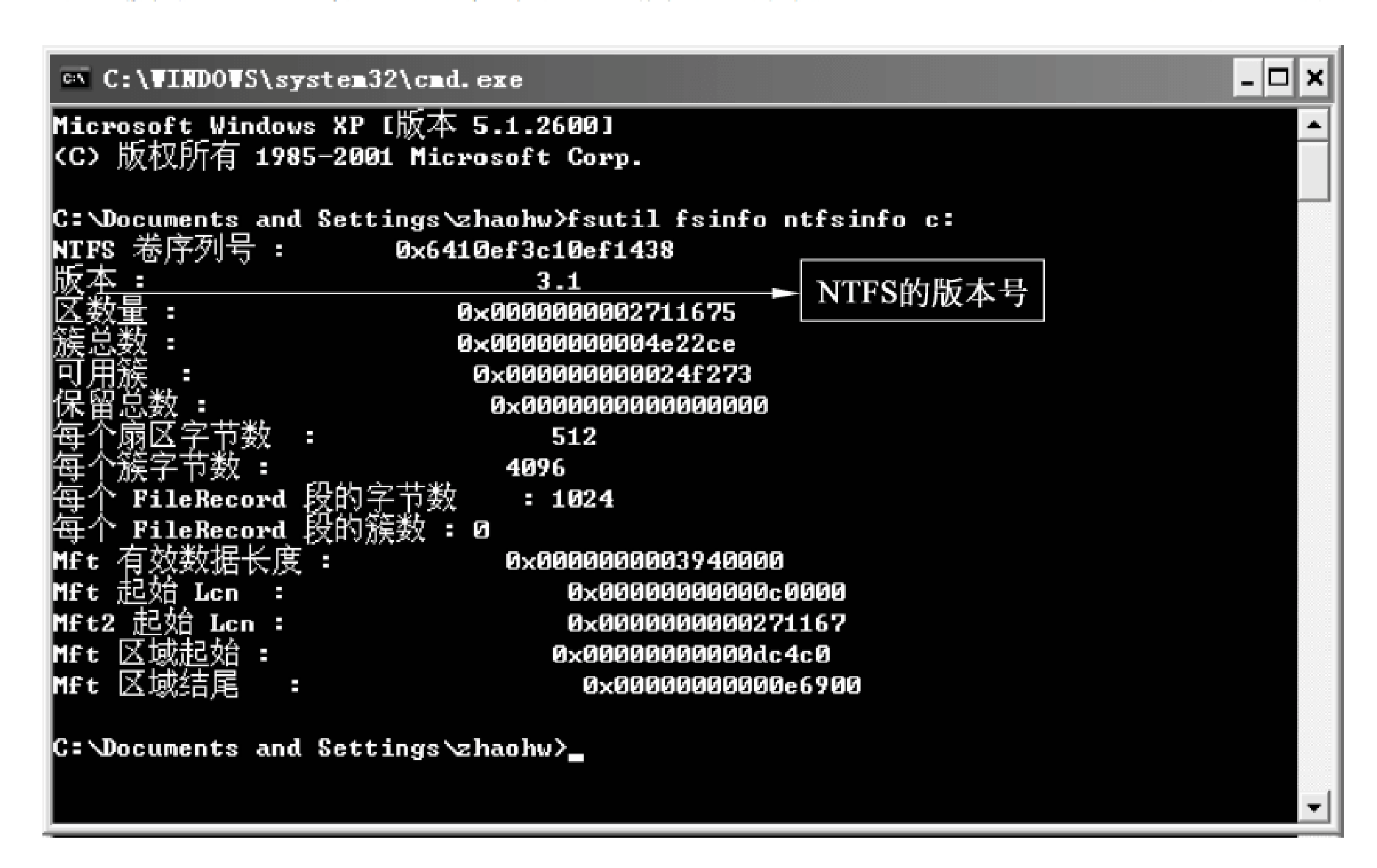


图 4.2 查看 NTFS 的版本号

4.5.2 将 FAT 文件系统转化为 NTFS 文件系统

Windows 系统提供了两种将 FAT 文件系统转化为 NTFS 文件系统的方式，即命令行

方式与图形界面方式。其中命令行方式下的转换可保证原有数据不丢失。

1. 命令行方式

① 单击“开始”→“运行”命令。

② 在弹出的“运行”对话框中输入 cmd 命令，然后单击“确定”按钮。

③ 在弹出的 cmd.exe 窗口中输入：“convert ＜需要转换的盘符＞/ fs:ntsf”，并敲击 Enter 键。此时若显示提示信息：“文件系统的类型是 FAT32”，由于该卷正在被另一个过程使用，“转换”不能进行。如果先卸下该卷，“转换”也许可以运行。该卷所有已打开的句柄将会无效。“要强制卸下该卷吗？（Y/N）”。输入“N”，会显示提示信息：“转换过程不能独占＜需要转换的盘符＞驱动器的访问，所以现在不能转换。是否重新计划转换过程，以便在系统下次重启时进行转换（Y/N）？”，若要继续进行转换，则输入“Y”，此时会显示提示信息“下一次重新启动系统时，转换操作会自动运行。”当计算机系统重启时，会自动进行 FAT 文件格式到 NTFS 文件格式的转换。

2. 图形界面方式

图形界面方式下的转换是采用格式化的方法将 FAT 文件系统的分区格式化为 NTFS 文件系统的分区。注意：在这种转化方式下，分区中的所有文件将会被删除，无法恢复，因此需谨慎操作。

① 在桌面上双击“我的电脑”，在打开的窗口中右键单击需要转换的盘符，在弹出的快捷菜单中选择“格式化”命令。如图 4.3 所示。



图 4.3　选择“格式化”操作

② 在弹出“格式化”对话框后，将其中的选项“文件系统”设置为 NTFS，然后单击“开始”按钮，则系统开始进行格式化，如图 4.4 所示。

注：Windows 系统没有提供内置的将 NTFS 文件系统转换为 FAT 文件系统的命令，如果需要进行这种转换，需要借助于第三方软件。但目前此类软件不宜在中文环境的 Windows 系统中实施转换，否则容易导致中文文件名的乱码现象。



图 4.4 “格式化 2003”对话框

4.5.3 NTFS 权限设置

首先使用 net user 命令新建一个用户：User1，如图 4.5 所示。

在一个 NTFS 分区上创建一个测试文件夹，并在文件夹中创建一个文本文件。进行 NTFS 权限设置，要求 user1 用户只能读取该文件夹。



图 4.5 创建新用户

在 NTFS 文件系统上，文件或文件夹的属性中有一个安全选项卡，可用于用户访问文件的权限设置。右击上述创建的测试文件夹，在弹出的快捷菜单中选择“属性”，可以打开“测试文件夹属性”对话框，选择“安全”选项卡，如图 4.6 所示。

图 4.6 的用户列表中列出了可以访问该文件或文件夹的所有用户和组。用户列表下方的文件夹权限列表中可以查看 NTFS 赋予用户操作该文件夹的所有权限。

此外，还应注意没有列出来的用户(属于该选项中列出的某个组)也可能具有对文件或文件夹的访问许可权。因此，最好不要把对文件的访问许可权分配给单个用户，而把许可权分配给组，然后把用户添加到组中，当需要更改访问权限时，只需更改整个组的访问许可权

即可，不必逐个更改每个用户的访问许可权(要更改访问权限，用户必须是所有者或已经由所有者授权执行该操作)。无论对文件和子文件夹的权限如何，被准许对文件夹进行完全控制的组或用户都可以删除该文件夹内的任何文件和子文件夹。

下面，可设置user1对测试文件夹的访问权限。首先在用户列表中添加user1：单击"安全"选项卡右边的"添加"按钮，在弹出的"选择用户或组"对话框中选择user1，单击"添加"按钮，当下面的显示框中出现"WINXP\USER1"时，单击"确定"按钮，如图4.7所示。



图4.6 "安全"选项卡

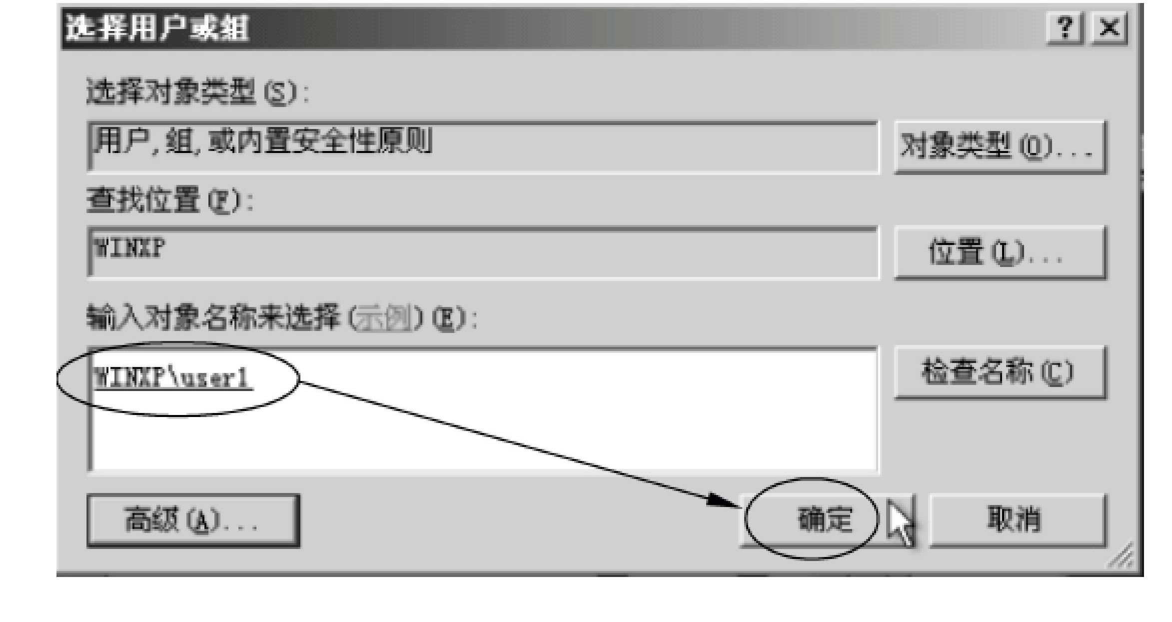


图4.7 选择user1

这样user1就出现在测试文件夹的用户列表中。选中user1，在权限列表中为它设置权限。根据实验要求，仅赋予它"读取"的权限，所以在权限列表中，选中"读取"后面的第一个复选框，如图4.8所示。

完成权限设置后注销administrator用户，再以user1登录。尝试在测试文件夹里新建文件夹，会弹出如图4.9所示的对话框，这证明user1只有读取的权限，而没有写入的权限。

备注：

Windows XP中常用的组和用户有：

- Administrators 内置管理员组，可以执行操作系统所支持的所有功能，对所有子文件夹和文件都具有完全控制权限。
- Users 普通用户组，此组代表计算机上所有的用户，默认权限是读取和运行/特殊权限。
- Guests 来宾组，与普通Users的成员有同等访问权，但来宾账户的限制更多。
- SYSTEM 此账户是代表操作系统本身，



图4.8 设置user1的权限



图 4.9 拒绝"写"操作

默认权限是完全控制。

- Everyone 所有用户,计算机上的所有用户都属于这个组。在 NTFS 磁盘格式中,默认将普通文件的所有访问权限均分配该组。若要对普通文件进行权限控制,则首先需要将 Everyone 从该文件的访问组中删除。选中 Everyone,单击右边的"删除"按钮即可。

4.6 实验思考

在 NTFS 文件系统上创建一个 temp.txt 文件,删除所有用户对它的访问权限,然后尝试打开 temp.txt 文件,查看操作结果。

实验5 安全登录

5.1 实验目的与要求

- 掌握 Windows 2000/NT 的登录及身份认证过程。
- 理解 SID、访问令牌、SAM 的含义。
- 掌握查看用户 SID 的方法。
- 掌握创建一个具有管理员权限的隐藏账户的方法。

5.2 实验环境

Windows 2000 操作系统。

5.3 预备知识

5.3.1 登录及身份认证过程

Windows 2000 必须确定自己是否在与合法的安全主体(即合法的用户)打交道,这是通过认证实现的,其中最简单的例子就是用户的登录及身份认证过程,如图 5.1 所示。一个成功的 Windows 登录过程要经过以下 4 个步骤。

(1) 用户按 Ctrl+Alt+Del 组合键,引起硬件中断,被系统捕获,这样使操作系统激活 WinLogon 进程(这是一个登录进程)。WinLogon 进程通过调用标识与鉴别 DLL,将登录窗口(账号名和口令登录提示符)展示在用户面前,要求用户输入一个用户名和口令。

(2) WinLogon 将用户名和口令传递给本地安全认证(Local Security Authority,LSA)。

(3) LSA 查询安全账号管理器(Security Account Manager,SAM)数据库,以确定用户名和口令是否属于授权的系统用户。如果用户名和密码合法,SAM 把该用户的 SID 以及该用户所属的所有组的 SID 返回给 LSA。LSA 使用这些信息创建一个访问令牌(Access Token),每当用户请求访问一个受保护资源时,LSA 就会将访问令牌显示出来以代表用户的"标记"。

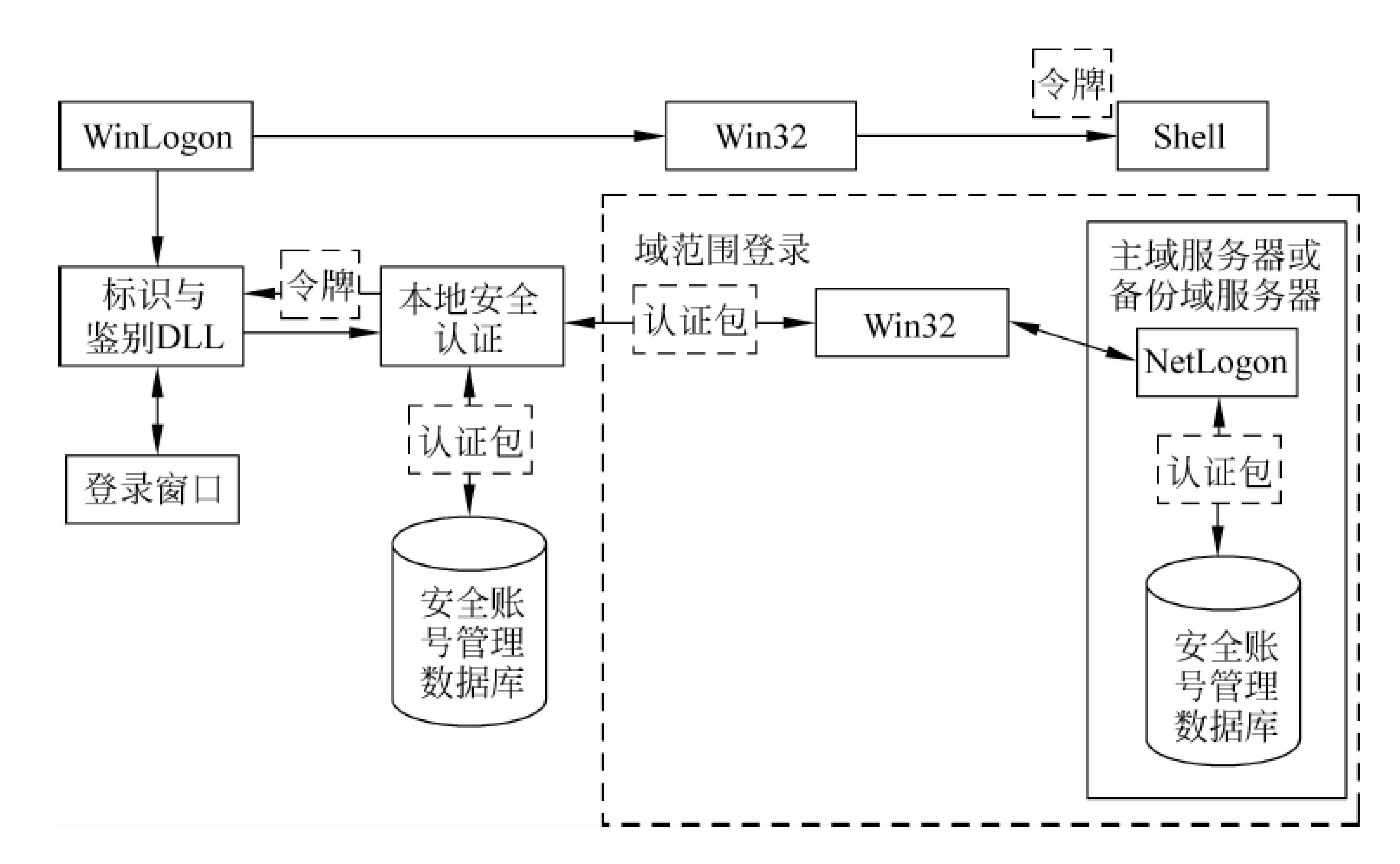


图 5.1　Windows 登录及身份认证过程

(4) WinLogon 进程传送访问令牌到 Win32 模块，同时发出一个请求，以便为用户建立登录进程。登录进程建立用户环境，包括启动 Desktop Explorer 和显示背景等。

5.3.2　SID

SID(Security Identifiers，安全标识符)用于在系统中唯一标识对象，在对象创建时由系统分配，包括域的 SID 和 RID(Relative Identifier，相对标识符)。原理上如果账户无限制增加的时候，会产生同样的 SID，但在通常情况下 SID 是唯一的。这种唯一性是由创建时的计算机名、系统时间、进程所消耗 CPU 的时间三要素共同确保的。

Windows 系统中的内部进程将引用账户的 SID 而不是账户的用户名或组名。如果创建一个账户，再删除该账户，那么即使再添加一个相同名称的账户，这个新账户也不会继承原账户的权限、权利与组的关系，因为它们具有不同的 SID。但是，重命名一个账户，即将该账户改名，由于 SID 并没有改变，因此其账户的属性、权限设置与组关系都不会受影响。

5.3.3　SAM

SAM(Security Account Manager，安全账号管理器)是控制和维护安全账号管理数据库，即 SAM 数据库的安全组件。该数据库包含所有用户和组的账号信息，包括密码 HASH、账户的 SID 等。安全账号管理器提供用户登录认证，负责对用户输入的信息与 SAM 数据库的信息对比，并为用户赋予一个 SID。

SAM 数据库位于注册表 HKLM\SAM\SAM 下，受到 ACL 保护，可以使用 regedt32.exe 打开注册表编辑器，通过设置适当权限来查看 SAM 中的内容。SAM 数据库在磁盘上就保存在%systemroot%system32\config\目录下的 sam 文件中，在这个目录下还包括一个 security 文件，是安全数据库的内容，两者密切相关。

5.3.4 访问令牌

用户通过验证后，登录进程会给用户一个访问令牌(Access Token)，该令牌相当于用户访问系统资源的凭证，它包括用户和这个用户属于的所有组的SID。当用户试图访问系统资源时，将访问令牌提供给Windows，然后Windows检查用户试图访问对象上的访问控制列表。如果用户被允许访问该对象，Windows将会分配给用户适当的访问权限。

访问令牌是用户在通过验证的时候有登录进程所提供的，所以改变用户的权限需要注销后重新登录，重新获取访问令牌。

5.4 实验内容

本章的实验内容包括以下3部分：

(1) 演示如何查看管理员用户的SID号。

(2) 演示如何创建一个新的普通用户，并通过查看该用户的SID号来分析管理员账号与普通账号的区别。

(3) 演示如何通过注册表操作来创建一个具有管理员权限的隐藏账号。

5.5 实验步骤

5.5.1 查看管理员用户的SID

可以使用whoami这样的工具(包含在Windows 2000 Resource Kit中)来查看与登录会话相关的SID。具体做法是：

① 在桌面上单击“开始”→“运行”命令，在弹出的“运行”对话框中输入cmd，然后单击“确定”按钮，会打开命令提示符窗口。

② 在闪烁的光标处输入whoami/? 命令，查看命令的所有功能。

③ 输入whoami /user命令，可查看用户的SID，如图5.2所示。

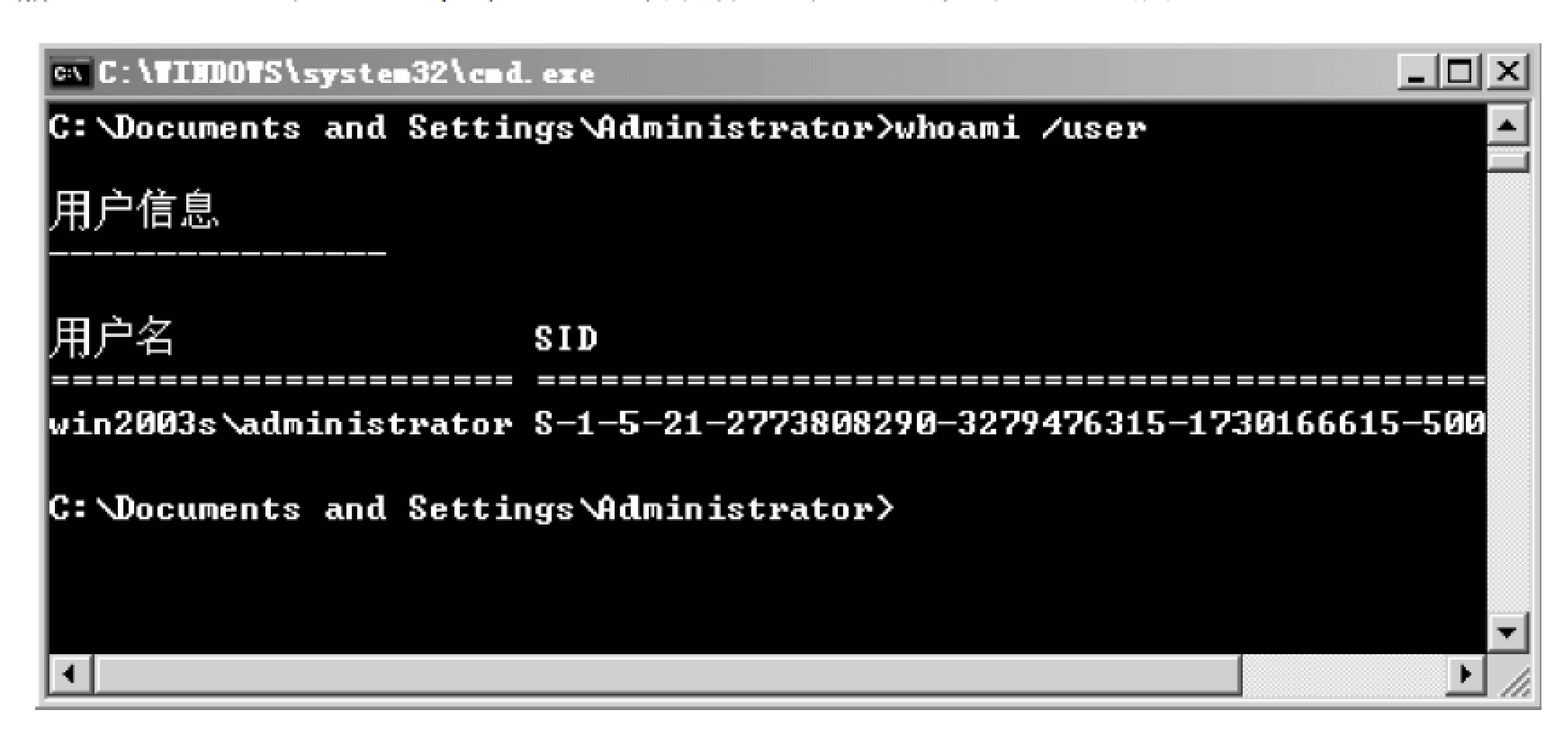


图5.2 查看管理员用户的SID

从图中可以看到，输入 whoami /user 命令后，可以查看到用户名为 administrator 的用户的 SID 为 S-1-5-21-2773808290-3279476315-1730166615-500。从此可以看到 SID 带有前缀 S，它的各个部分之间用连字符隔开。第一个数字(本实验中的 1)是修订版本号；第二个数字是标识符颁发机构代码(对 Windows 2000 来说总是为 5)；然后是 4 个子颁发机构代码(本例中是 21 和后续的 3 个长数字串)和一个相对标识符(Relative Identifier，RID，本实验中是 500)。SID 中的一部分是各系统和域唯一具有的，而另一部分(RID)是跨所有系统和域共享的。当安装 Windows 2000 时，本地计算机会颁发一个随机的 SID。类似的当创建一个 Windows 2000 域时，它也被指定一个唯一的 SID。于是对任何的 Windows 2000 计算机或域来说，子颁发机构代码总是唯一的(除非故意修改或复制，例如某些底层的磁盘复制技术)。RID 对所有的计算机和域来说都是一个常数。例如，带有 RID 500 的 SID 总是代表本地计算机的真正的 Administrator 账户，RID 501 是 Guest 账户。

5.5.2 查看新建用户的 SID

① 在命令提示符窗口的闪烁光标处输入 net user Tuser/add 命令，添加用户名为 Tuser 的新用户，如图 5.3 所示。

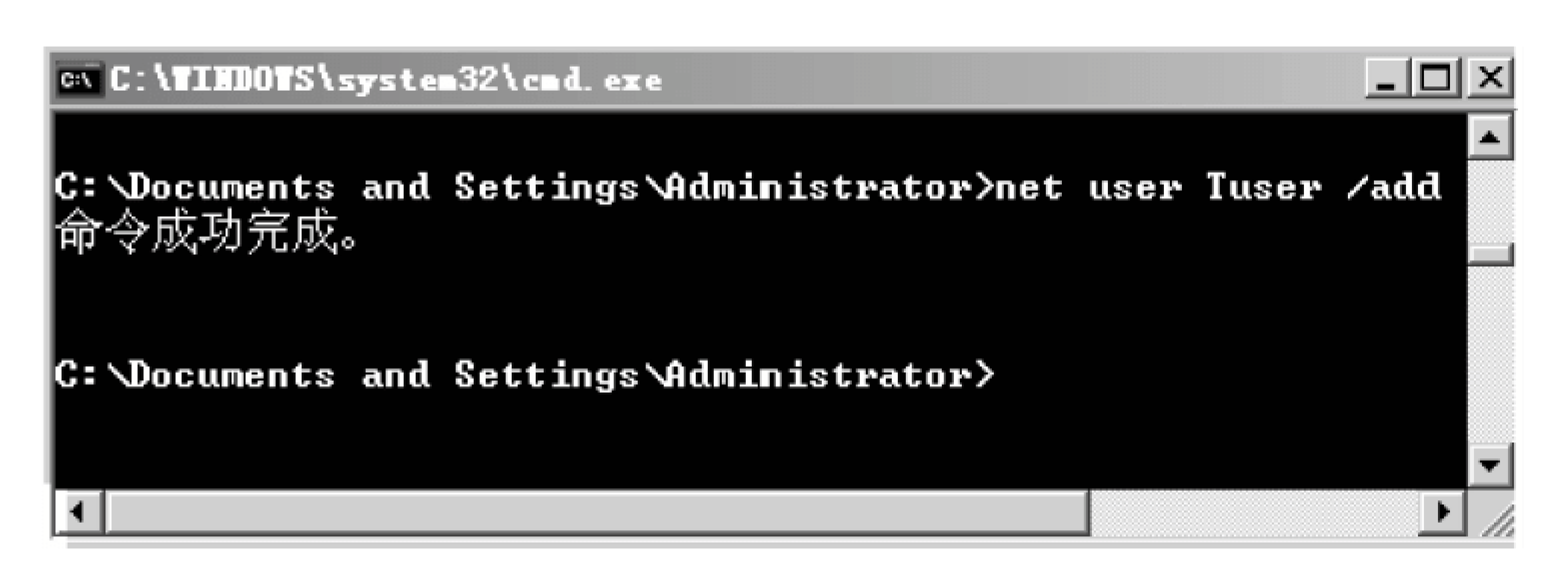


图 5.3 添加用户 Tuser

② 用户新建成功后，注销管理员用户，以 Tuser 用户的身份重新登录 Windows。

③ 重新打开命令行窗口，在命令提示符窗口的闪烁光标处再次输入 whoami /user 命令，可看到用户名和用户 SID 都改变了。用户名为 tuser(用户名的大小写无关)；用户 SID 为 S-1-5-21-2773808290-3279476315-1730166615-1010，如图 5.4 所示。由此可以看出用户 Tuser 的 RID 与 administrator 的 RID 不同。在域中，从 1000 开始的 RID 代表用户账户



图 5.4 查看用户 Tuser 的 SID



（例如，本实验中 RID 1010 是在该域中创建的第 9 位用户），Windows 2000（或者使用适当工具的恶意黑客）总是将具有 RID 500 的账户识别为管理员。

5.5.3 创建一个具有管理员权限的隐藏账户

在前面的预备知识中已经大致介绍了 SAM 和 SID 的相关知识，利用这些知识我们来创建一个具有管理员权限的隐藏账户，必要时将对 SAM 数据库做进一步阐述。

1. 打开注册表

① 注销 Tuser 用户，以用户 administrator 的身份重新登录 Windows 操作系统。

② 在桌面上单击"开始"→"运行"命令，在弹出的对话框中输入 regedit 命令，然后单击"确定"按钮，打开注册表。在 HKLM\SAM\SAM\domains\account\下找到用户 administrator 和 Tuser，如图 5.5 所示。

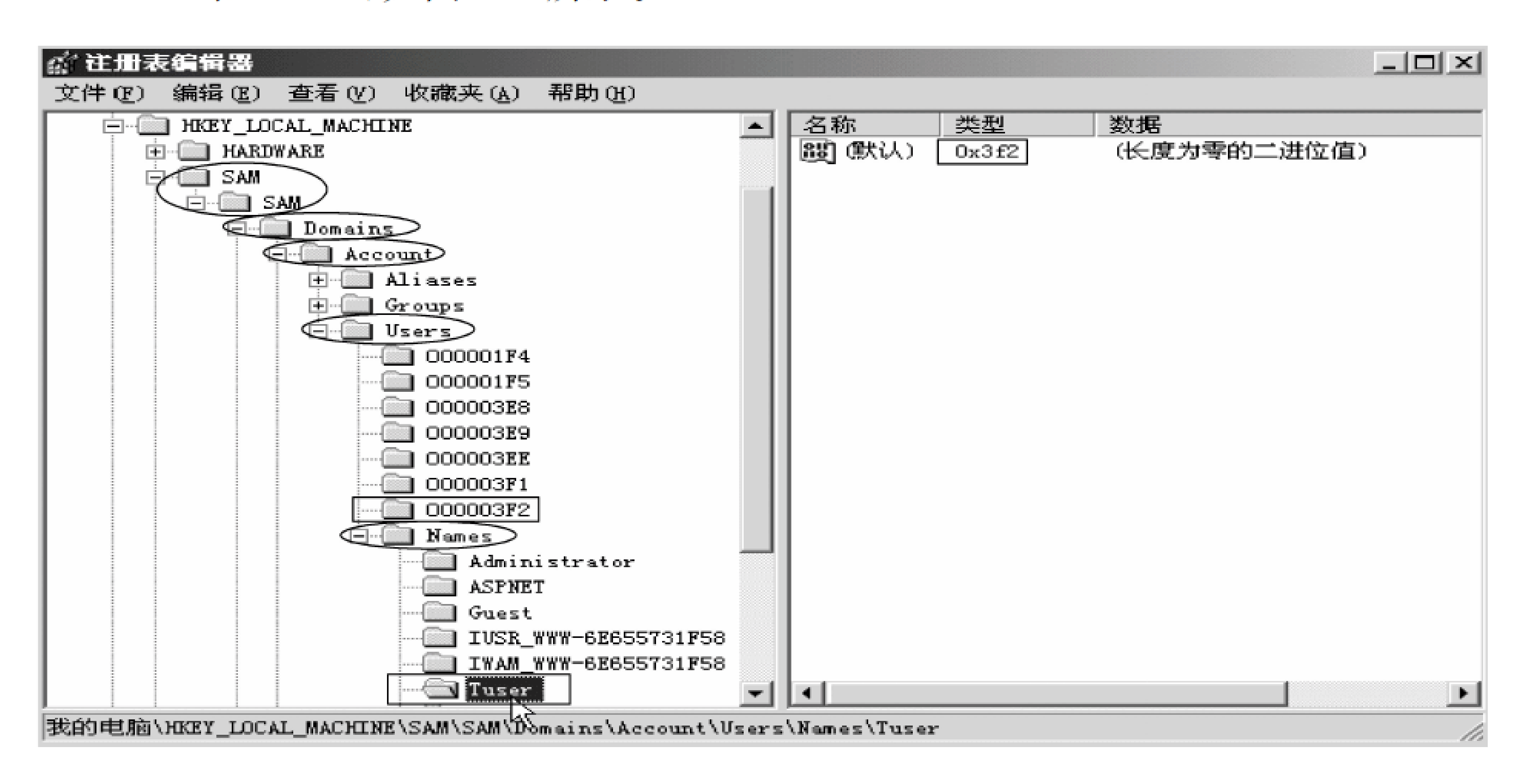


图 5.5 注册表编辑器窗口

SAM 数据库位于注册表 HKLM\SAM\SAM 下，受到 ACL 保护，它在磁盘上保存在"%systemroot%system32\config\"目录下的 sam 文件中。在\Domains\中的为域（或本机）中的 SAM 内容，其下有两个分支"Account"和"Builtin"，其中\Domains\Account 是用户账号内容：

- \Domains\Account\Users 下是各个账号的信息。其下的子键就是各个账号的 SID 相对标识符。比如 000001F4 是管理员 RID。
- \Domains\Account\Names\下是用户账号名，每个账号名只有一个默认的子项，项中类型不是一般的注册表数据类型，而是指向标志这个账号的 SID 相对标识符，比如其下的 Administrator，类型为 0x1f4，于是\Domains\Account\Users 中的 000001F4 就对应着账户名 Administrator 的内容。再例如本实验中的 Tuser，类型为 0x3f2，于是\Domains\Account\Users 中的 000003F2 就对应着账户名 Administrator 的内容（如图 5.5 中红色方框中的内容），依此类推。

值得注意的地方是：默认情况下管理员无法直接访问 SAM 数据库，要查看它使用 RegEdt32 修改 SAM 访问权限，或者使用 psu、wsu 启动 system 权限的 regedit。因此本实验中的 SAM 也必须赋予完全控制权限。具体操作过程是：在注册表编辑器窗口中右键单击 SAM 文件夹下的 SAM 子文件夹，在弹出的快捷菜单中选择"权限"命令，在弹出的"SAM 权限"对话框中，选择 Administrator 用户，在它的权限列表中，选中"完全控制"的"允许"复选框，如图 5.6 所示。

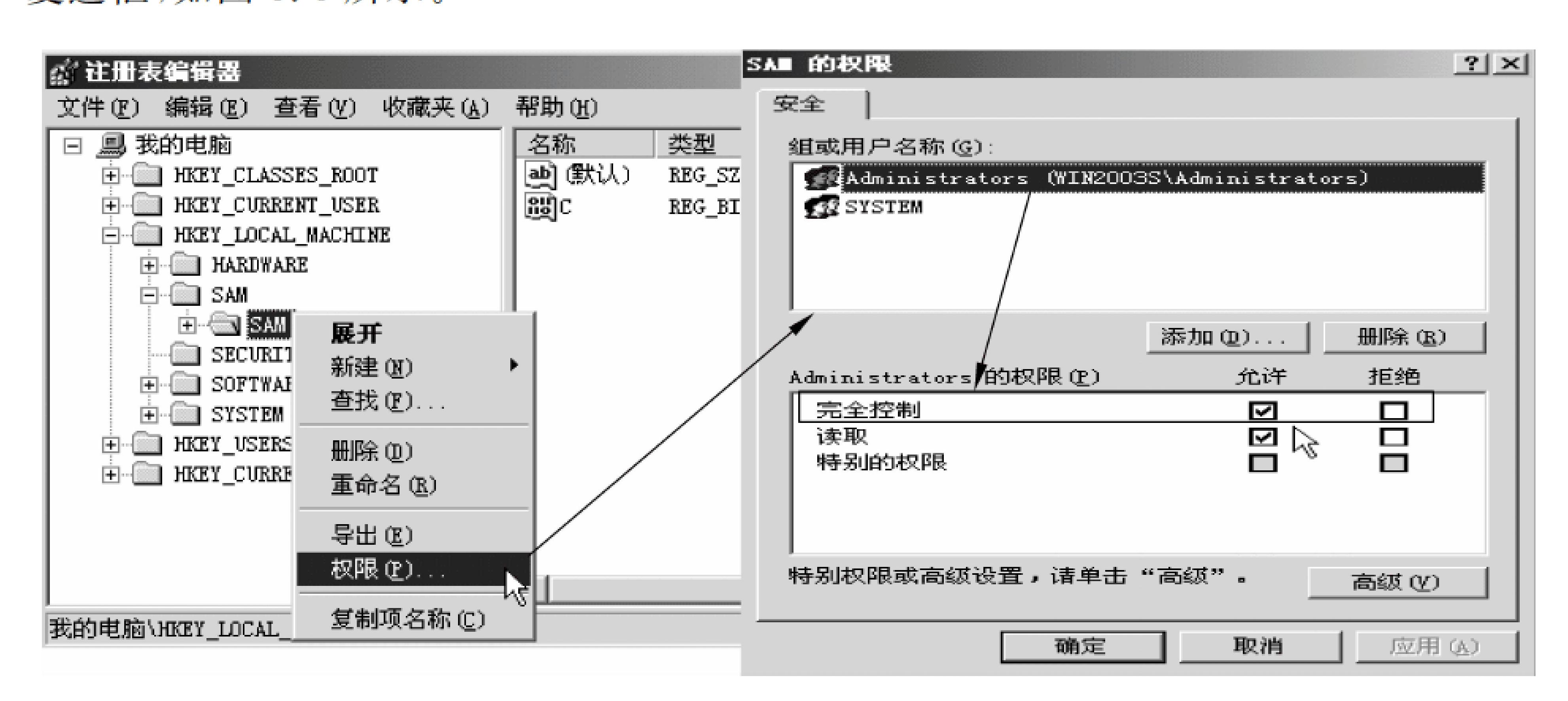


图 5.6 为 SAM 赋予完全控制权限

2. 复制 F 项

上一小节中提到：\Domains\Account\Users 下存放着各个账号的信息，其中每个账号下面有两个子项，F 项和 V 项。

- 项目 V 中保存的是账户的基本资料，用户名、用户全名(full name)、所属组、描述、密码 hash、注释、是否可以更改密码、账户启用、密码设置时间等。
- 项目 F 中保存的是一些登录记录，比如上次登录时间、错误登录次数等，还有一个重要的地方就是这个账号的 SID 相对标识符。

因此，要创建一个具有管理员权限的隐藏账户，就必须复制 Administrator 用户的 F 项内容到某一账户。具体做法是：选中 Users 文件夹下 000001F4 子文件夹(上一小节已经说明，这个子文件夹就对应于 Names 文件夹下的 Administrator 子文件夹)的 F 项，单击右键，在弹出的快捷菜单中选择"修改"命令，复制其中的内容到 User 文件夹下 000003F2 子文件夹(上面 1. 中已经说明，这个子文件夹就对应于 Names 文件夹下的 Tuser 子文件夹)的 F 项中，如图 5.7 所示。

3. 查看修改后用户 Tuser 的 SID

注销 Administrator 用户，以用户 Tuser 的身份重新登录 Windows 操作系统。重复 2 中的操作，查看用户 Tuser 的 SID，如图 5.8 所示。比较图 5.1、图 5.4 和图 5.8 会发现用户 Tuser 的 SID 发生了变化，它的 RID 由 1010 变成了 500，具有了管理员权限；至此用户 Tuser 与管理员用户 Administrator 的 SID 变得完全一样了。

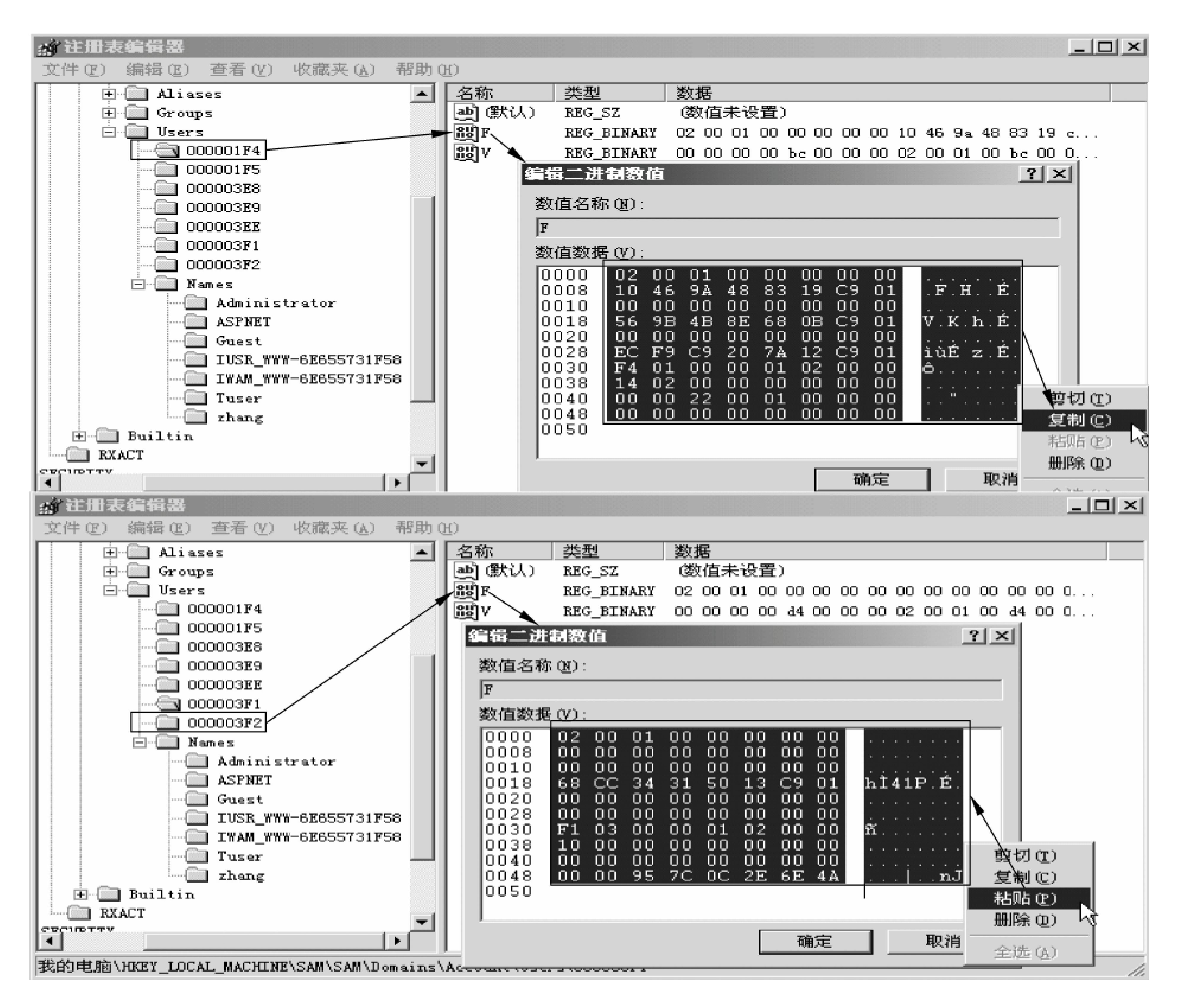


图 5.7 复制 F 项中的内容

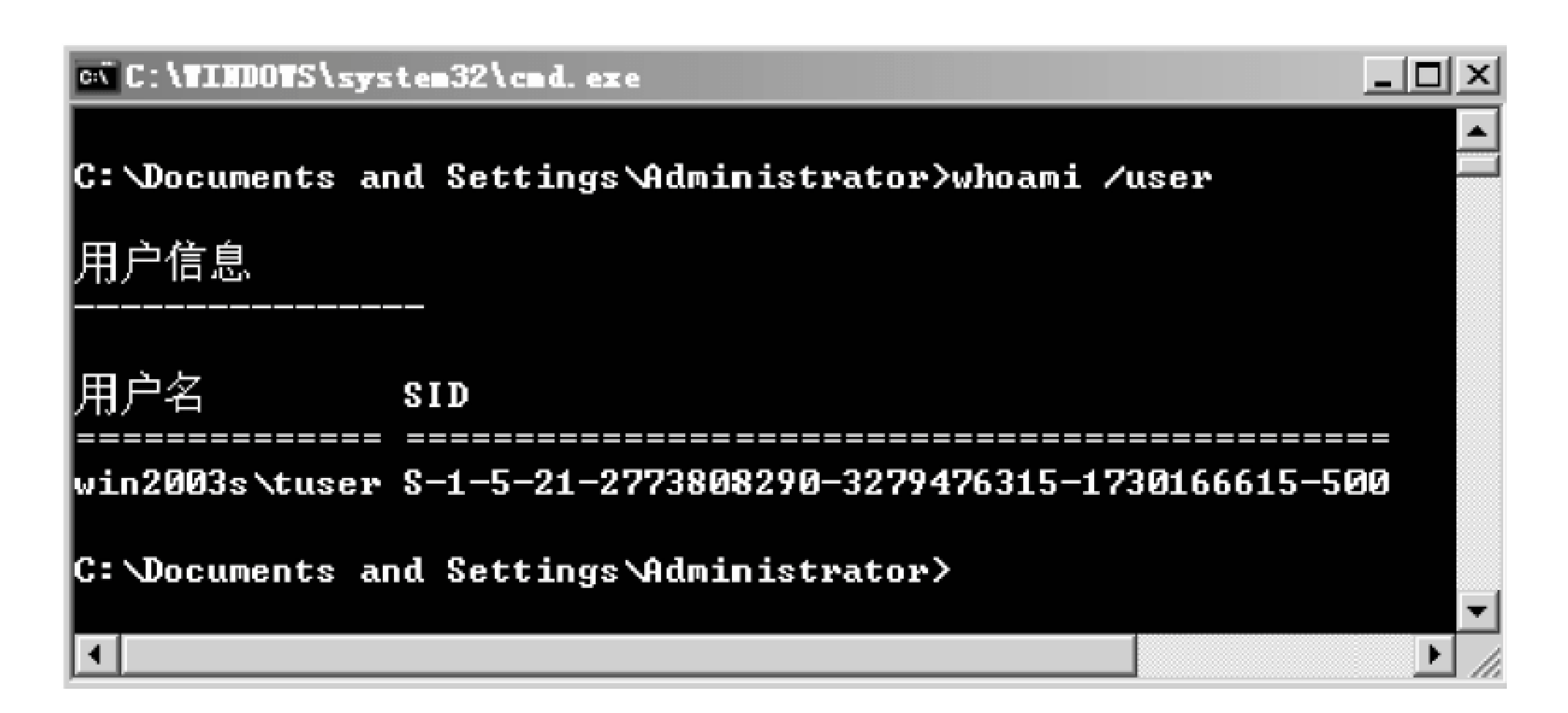


图 5.8 再次查看用户 Tuser 的 SID

4. 将 Tuser 的注册表导出,在图形界面下删除 Tuser,然后导入注册表

再次注销 Tuser 用户,以用户 Administrator 的身份重新登录 Windows 操作系统。在桌面上单击"开始"→"运行"命令,在弹出的对话框中输入 regedit 命令,然后单击"确定"按钮,打开注册表。在 HKLM\SAM\SAM\domains\account\下找到用户 Tuser,分别将它在

Names 下的子文件夹 Tuser 和所对应的在 user 下的子文件夹 000003F2 导出，暂存到“我的文档”中，命名为 1.reg 和 2.reg，具体操作(以 Tuser 字文件夹为例)如图 5.9 所示。

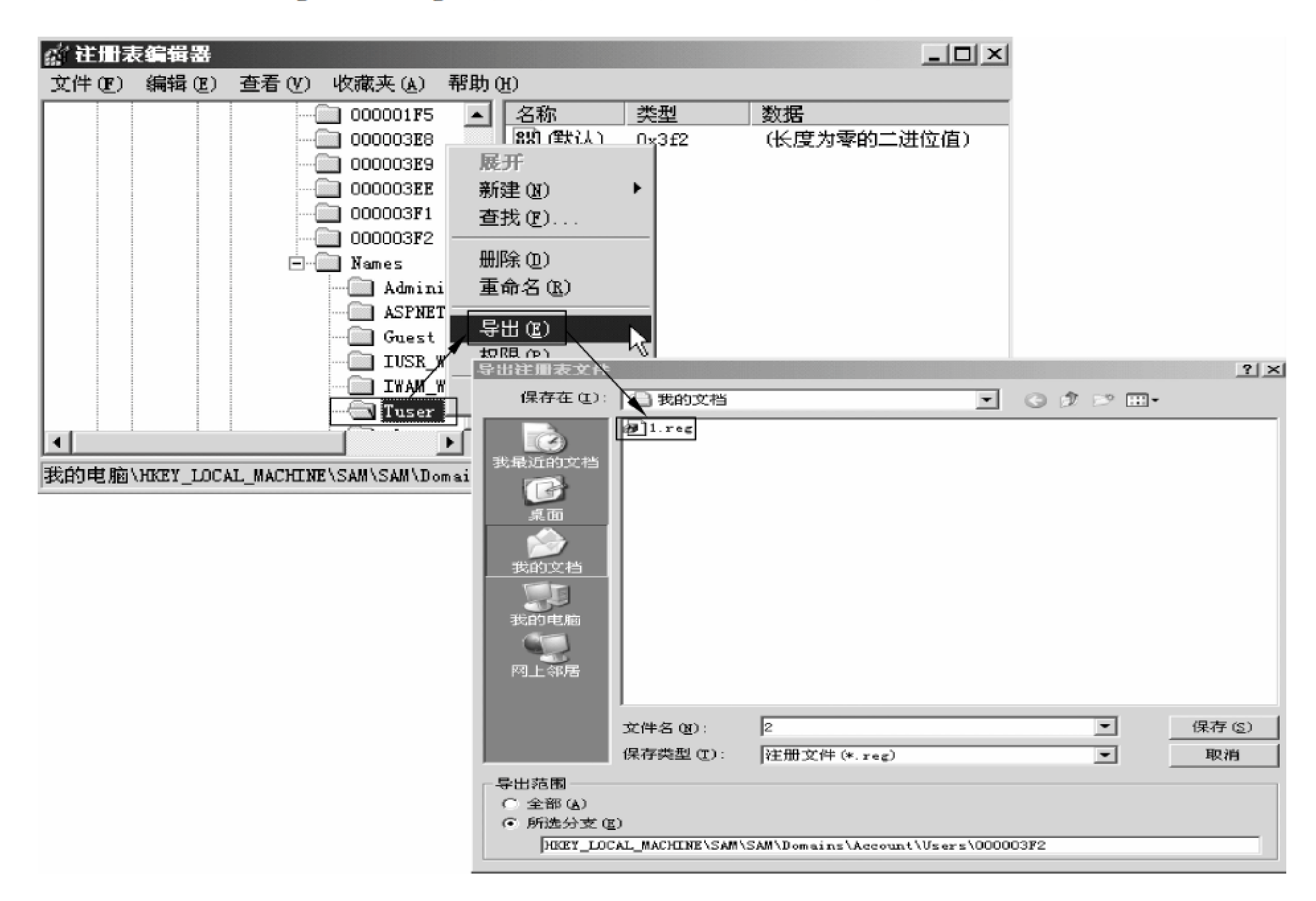


图 5.9 导出注册表中的 Tuser 子文件夹

回到“桌面”，右键单击“我的电脑”，在弹出的快捷菜单中选择“管理”命令，在“计算机管理”窗口中单击“本地用户和组”目录下的“用户”字文件夹，在右边窗口的用户列表中右击 Tuser 用户，在弹出的快捷菜单中选择“删除”命令，如图 5.10 所示。



图 5.10 删除 Tuser 用户

再次打开注册表后，会发现\Domains\Account\Names\下的子文件夹 Tuser 和所对应的在\Domains\Account\User 下的子文件夹 000003F2 不可访问，如图 5.11 所示。



图 5.11　Tuser 用户的相应子文件夹已被删除

打开“我的文档”，将导出的注册表文件 1.reg 和 2.reg 双击导入注册表。再次打开注册表后，会发现\Domains\Account\Names 下的子文件夹 Tuser 和所对应的在\Domains\Account\User 下的子文件夹 000003F2 可以访问，如图 5.12 所示。

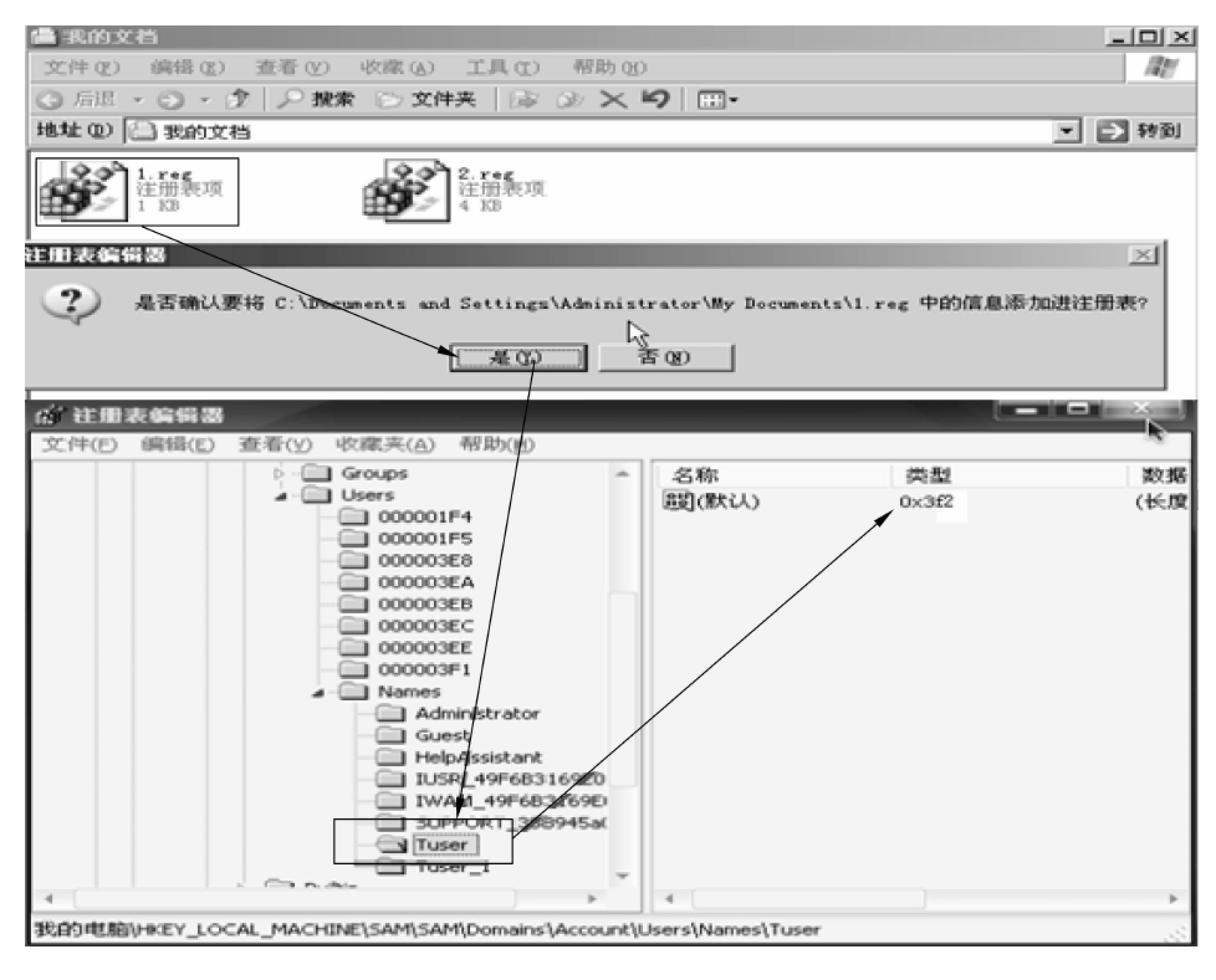


图 5.12　在注册表中重新导入 Tuser 用户的相应子文件夹

再次回到“桌面”，右键单击“我的电脑”→“管理”→“本地用户和组”→“用户”，却找不到用户 Tuser，至此一个隐藏的具有管理员权限的账户就已经建立了，如图 5.13 所示。

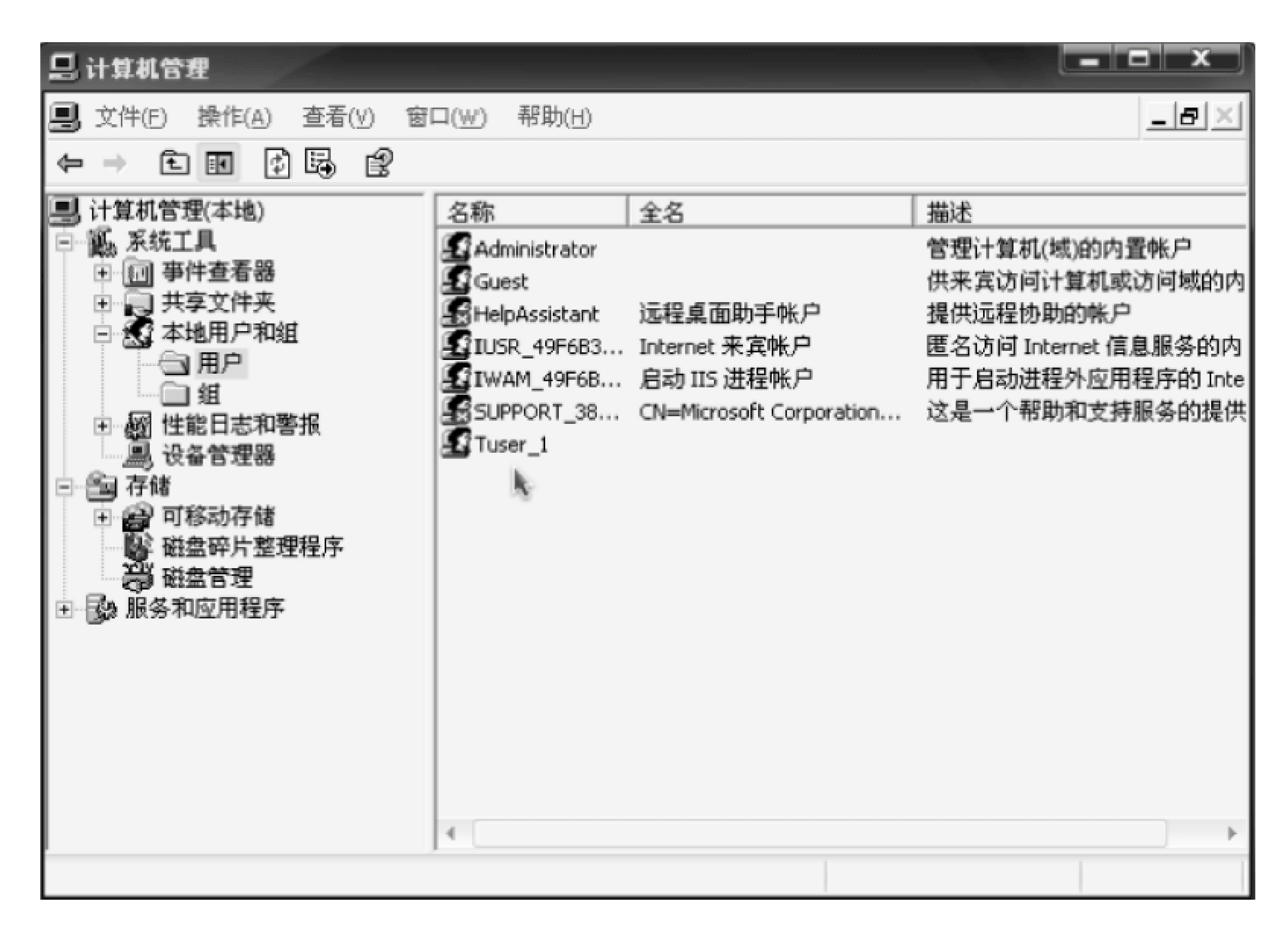


图 5.13 用户 Tuser 已被删除

至此，可以看出，本实验之所以可以克隆一个具有管理员权限的用户，是因为 SID 的相对标识符 RID 在注册表中的一个账号中出现了两遍，一个是在子键 000001F4 中，另一个地方就是子键中 F 项的内容里面，从 48 到 51 的四个字节：F4 01 00 00，这实际上是一个 long 类型变量，也就是 00 00 01 F4。当一个标识出现在两个地方的时候就将发生同步问题。显然，微软犯了这个毛病。两个变量本应该统一标识一个用户账号，但是微软把两个变量分别发挥各自的作用，却没有同步统一起来。Windows 登录时，将从 SAM 中获得相对标识符，而这个相对标识符的位置是 F 值中的 F4 01 00 00。但是，账户信息查询却是使用 SAM 中 Names 子键的内容。

需要指出的是，SAM HACK 是非常有危险性的。不正确的修改会将系统的安全数据管理器破坏，造成系统启动问题。

5.6 实验思考

(1) 在命令行界面中使用 net user 命令创建一个 test 账号，查看并记录其 SID 号，然后将 test 账号删除并重新创建一个 test 账号，观察两次 test 账号对应的 SID 号是否一致。

(2) 观察一下 Windows 2000、Windows 2003、Windows XP 以及 Windows 7 等不同版本的 Windows 系统中，adiministrator 账号的 SID 号是否相同。



实验6 Windows 账户与口令的安全设置

6.1 实验目的与要求

- 掌握 Windows 操作系统中安全账户的设置方法。
- 掌握 Windows 操作系统中高强度登录密码的设置方法。
- 掌握利用 SYSKEY 保护账户信息的方法。

6.2 实验环境

Windows XP 操作系统。

6.3 预备知识

6.3.1 Windows 的域安全策略

目前常见的安装在服务器端的 Windows 操作系统中均带有"域安全策略",这是一种非常有效的系统安全管理工具。可以通过依次单击"开始"→"设置"→"控制面板"→"管理工具"→"域安全策略"命令,打开"域安全策略"进行相关设置。Windows 的域安全设置可分为账户策略,本地策略、公钥策略、事件日志、受限制的组、系统服务、注册表、文件系统、公钥策略和 IP 安全策略。

(1) 账户策略是由用户名+密码组成,我们利用账户策略设置密码策略、账户锁定和 Kerberos(只针对域)策略。

(2) 本地策略。本地策略所设置的值只对本地计算机起作用,它包括审核策略、授予用户权限,设置各种安全机制。

(3) 事件日志。主要是对域(包括本地)的各种事件进行记录。为应用程序日志、系统日志和安全日志配置大小、访问方式和保留时间等参数。

(4) 受限制的组。管理内置组的成员资格。一般内置组都有预定义功能,利用受限制组可以更改这些预定义的功能。

(5) 系统服务。为运行在计算机上的服务配置安全性和启动设置。

(6) 注册表。配置注册密钥的安全性,在 Windows XP 中,注册表是

一个集中式层次结构数据库，它存储 Windows 所需要的必要信息，用于为用户、程序、硬件设备配置进行统计。

（7）文件系统。指定文件路径配置安全性。

（8）公钥策略。配置加密的数据恢复代理和信任认证中心证书。证书是软件服务证书，可以提供身份鉴定的支持，包括安全的 E-mail 功能，基于 Web 的身份鉴定和 SAM 身份鉴定。

（9）IP 安全性策略。配置 IPSec（IP 协议安全性）。IPSec 是一个工业标准，用于对 TCP/IP 网络数据流加密以及保护企业内部网内部通信和跨越 Internet 的 VPN（虚拟专用网络）通信的安全。

6.3.2 Windows 的本地安全策略

与之相对应的另一组 Windows 操作系统中带有“本地安全策略”，例如 Windows XP 操作系统。打开“本地安全策略”进行相关设置。顾名思义，域安全策略设置作用于整个域，而本地安全策略设置仅作用于本台计算机。本地安全策略包括 4 个子项目：“账户策略”、“本地策略”、“软件限制策略”与“IP 安全策略”，其中通过对“账户策略”与“本地策略”的设置，可有效保护 Windows 登录账户的安全性。本实验主要是通过对本地安全策略进行相应设置以提高操作系统账户和口令的安全。

6.3.3 Administrator 和 Guest 账户

“本地用户和组”位于“开始”→“设置”→“控制面板”→“管理工具”→“计算机管理”中，用户可以利用这一组管理工具来管理单台本地或远程计算机。可以使用“本地用户和组”保护并管理存储在本地计算机上的用户账户和组。可以在特定计算机和仅这台计算机上分配本地用户或组账户的权限和权利。

通过“本地用户和组”，可以为用户和组分配权利和权限，从而限制了用户和组执行某些操作的能力。权利可授权用户在计算机上执行某些操作，如备份文件和文件夹或者关机。权限是与对象（通常是文件、文件夹或打印机）相关联的一种规则，它规定哪些用户可以访问该对象以及以何种方式访问。

“本地用户和组”的“用户”文件夹显示了默认的用户账户以及操作系统用户所创建的用户账户。其中有两个特殊的账户：Administrator 和 Guest 账户。

Administrator 和 Guest 账户是在安装 Windows 时自动建立的账户，也称为内置账户。这两个账户在 Windows 安装之后已经存在并且被赋予了相应的权限，它们不能被删除（即使是管理员也不能），其中 Administrator 账户还不允许被屏蔽，开始时 Guest 账户处于停用状态。Administrator 和 Guest 账户的权限如下。

（1）Administrator。在域中和计算机中具有不受限制的权利，可以管理本地或域中的任何计算机，如创建账户、创建组、实施安全策略等。Administrator 账户具有对服务器的完全控制权限，并可以根据需要向用户指派用户权利和访问控制权限。Administrator 账户是服务器上 Administrators 组的成员。永远也不可以从 Administrators 组删除

Administrator 账户，但可以重命名或禁用该账户。由于大家都知道 Administrator 账户存在于许多版本的 Windows 上，所以重命名或禁用此账户将使恶意用户尝试并访问该账户变得更为困难。

（2）Guest。供在域中和计算机中没有固定账户的用户临时使用计算机或访问域。如果某个用户的账户已被禁用，但还未删除，那该用户也可以使用 Guest 账户。Guest 账户不需要密码。默认情况下，Guest 账户是禁用的，但也可以启用它。该账户在默认情况下不允许对计算机或域中的设置和资源做永久性改变。可以像任何用户账户一样设置 Guest 账户的权利和权限。默认情况下，Guest 账户是默认的 Guest 组的成员，该组允许用户登录服务器。其他权利及任何权限都必须由 Administrators 组的成员授予 Guests 组。

6.3.4 高强度登录密码

登录密码是目前 Windows 操作系统采用的，识别合法用户的一种常见有效手段，在保护 Windows 操作系统安全，避免非法用户入侵方面具有重要作用；若登录密码强度不够，那么整个操作系统的安全性将存在严重隐患。因此设置高强度的登录密码，并采用有效措施保护登录密码是保障计算机安全的一种基本手段。

一个高强度的密码至少要包括下列 4 方面内容的 3 种：

- 大写字母；
- 小写字母；
- 数字；
- 非字母数字的特殊字符，如标点符号等。

另外高强度的密码还要符合下列的规则：

- 不使用普通的名字、昵称或缩写；
- 不使用普通的个人信息，如生日日期；
- 密码不能与用户名相同，或者相近；
- 密码里不含有重复的字母或数字。

另外，在目前的 Windows 操作系统中，密码字符是 7 个一组进行存放的，密码破解工具在破解密码时通常是针对这种特点实施分组破解，因此密码的长度最好为 7 的整倍数。

6.3.5 SYSKEY

从 Windows NT4 Service Pack 3 开始，Microsoft 提供了对 SAM 散列值进行进一步加密的方法，称为 SYSKEY。SYSKEY 是 System KEY 的缩写，它生成一个随机的 128 位密钥，对散列值再次进行加密（请注意：不是对 SAM 文件加密，而是对散列值进行加密）。因此 SYSKEY 可以用来保护 SAM 数据库不被离线破解。用过去的加密机制，如果攻击者能够得到一份加密过的 SAM 库的拷贝，就能够在自己的机器上来破解用户口令。目前已经有一些专门用来破解 SAM 数据库的工具。SYSKEY 对数据库采用了更多的加密措施，目的是增加破解的计算量，使暴力破解从时间上考虑不可行。

6.4 实验内容

本章的实验内容主要包括以下3个部分：

(1) 演示如何对账户实施管理，以确保系统的安全性，其中包括限制用户数量、停用Guest账户、重命名管理员账户、设置双管理员账户和设置陷阱账户等几个部分。

(2) 演示通过设置本地安全策略中的密码策略和账户锁定策略来确保账户的安全性。

(3) 演示如何使用Windows系统自带的syskey工具来保护SAM文件中的账户信息。

6.5 实验步骤

6.5.1 账户设置

1. 限制用户数量

去掉所有的测试账户、共享账户等，尽可能少地建立有效账户，没有用的一律不要，多一个账户就多一个安全隐患。系统的账户越多，被攻击者攻击成功的可能性越大。因此，要经常用一些扫描工具查看系统账户、账户权限及密码，并且及时删除不再使用的账户。对于Windows主机，如果系统账户超过10个，一般能找出一两个弱口令账户，所以账户数量不要大于10个。

具体做法是：

① 依次单击“开始”→“设置”→“控制面板”命令，然后依次双击“管理工具”→“计算机管理”，弹出如图6.1所示的窗口。



图6.1 删除休眠账户

② 单击“本地用户和组”前面的“+”,然后单击“用户”,在右边出现的用户列表中,选择要删除的账户,单击右键,在弹出的快捷菜单中,选择“删除”命令,在接下来出现的对话框中,单击“是”按钮。

2. 停用 Guest 账户

将 Guest 账户停用,改成一个复杂的名称并加上密码,然后将它从 Guests 组删除,任何时候都不允许 Guest 账户登录系统。

具体做法是:

依次单击“开始”→“设置”→“控制面板”命令,然后依次双击“管理工具”→“计算机管理”,弹出如图 6.2 所示的窗口。

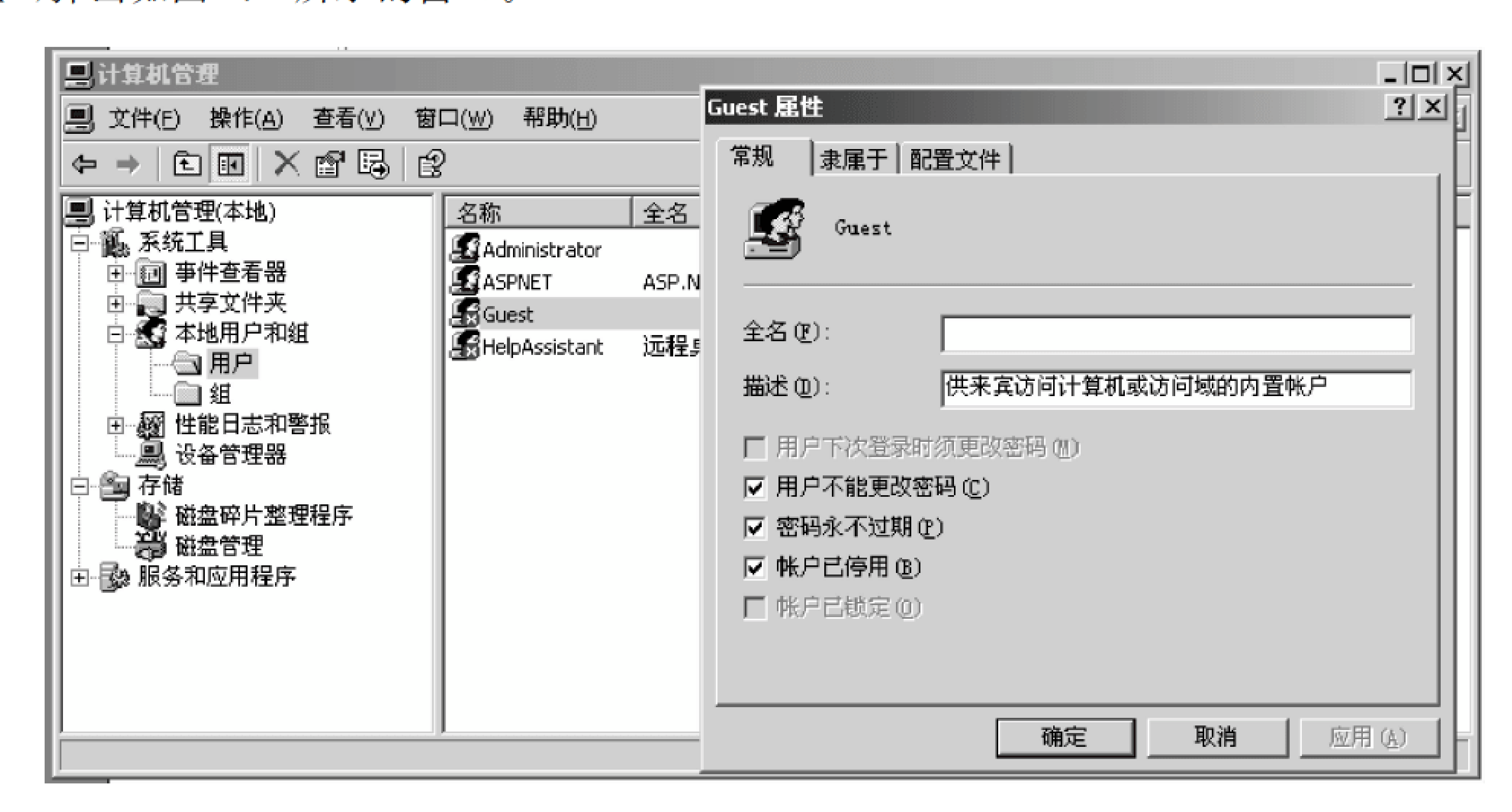


图 6.2 停用 Guest 账户

单击“本地用户和组”前面的“+”,然后单击“用户”,在右边出现的用户列表中,选择 Guest 账户,单击右键,在弹出的快捷菜单中,单击“属性”,在接下来出现的对话框中,选择“账户已停用”复选框。

然后,在同一个快捷菜单中单击“重命名”,为 Guest 起一个新名字;单击“设置密码”,设置一个复杂的密码。

接下来,单击“组”,在右边出现的组列表中,双击 Guests 组,在弹出的对话框中选择 Guest 账户,单击“删除”按钮。如图 6.3 所示。

3. 重命名管理员账户

用户登录系统的账户名对于黑客来说也有着重要意义。当黑客得知账户名后,可发起有针对性的攻击。目前许多用户都在使用 Administrator 账户登录系统,这为黑客的攻击创造了条件。因此可以重命名 Administrator 账户,使得黑客无法针对该账户发起攻击。但是注意不要使用 Admin,root 之类的特殊名字,要尽量伪装成普通用户,例如:user1。

具体做法有两种:

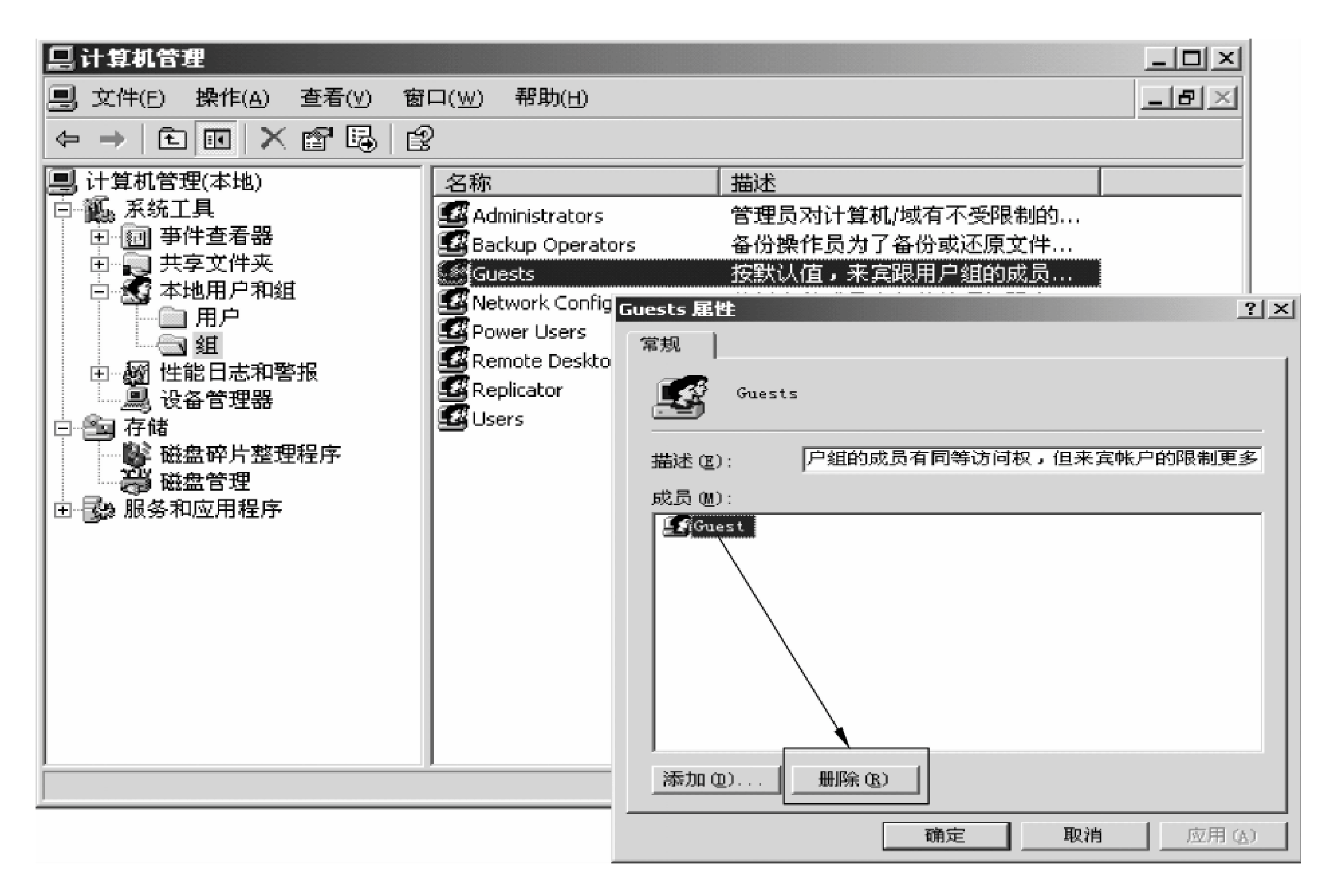


图 6.3　从 Guests 组中删除 Guest 账户

（1）依次单击“开始”→“设置”→“控制面板”，然后依次双击“管理工具”→“计算机管理”，在弹出的窗口中单击“本地用户和组”前面的“+”，然后单击“用户”，在右边出现的用户列表中，选择 Administrator 账户，单击右键，在弹出的快捷菜单中，单击“重命名”，在接下来出现的对话框中，为 Administrator 账户重命名。

（2）打开“本地安全策略”窗口，在窗口左侧依次选择“安全设置”→“本地策略”→“安全选项”，如图 6.4 所示。在窗口右侧双击选择“账户：重命名系统管理员账户”选项，在弹出的对话框中将更改 Administrator 账户名，如图 6.5 所示。

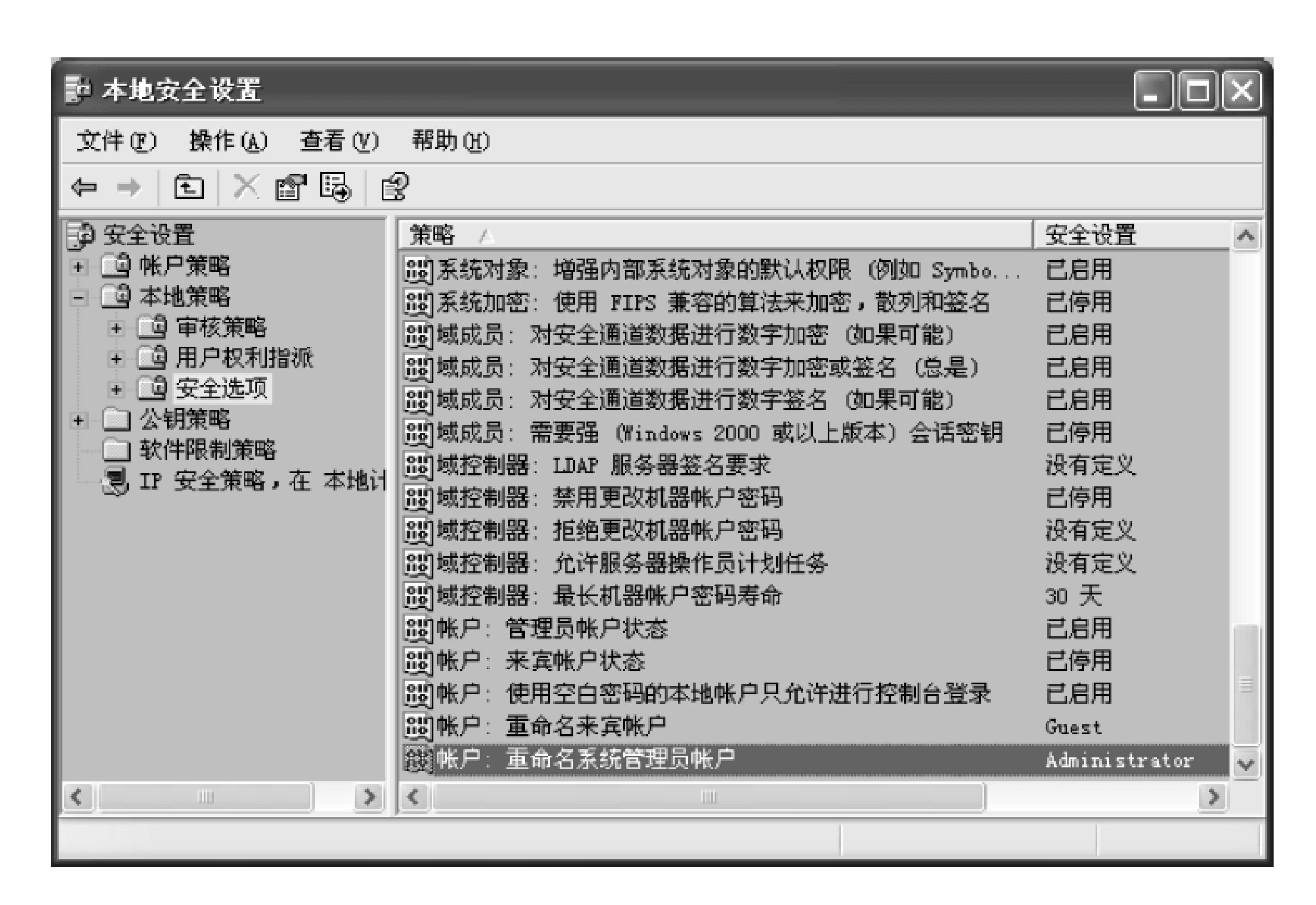


图 6.4　打开“安全选项”

4. 设置两个管理员账户

因为只要登录系统后，密码就存储在WinLogon进程中，当有其他用户入侵计算机的时候就可以得到登录用户的密码。所以可以设置两个管理员账户，一个用来处理日常事务，一个用作备用。



图 6.5 重命名管理员账户

5. 设置陷阱账户

在Guests组中设置一个Administrator账号，把它的权限设置成最低，并给予一个复杂的密码(至少要超过10位的超级复杂密码，而且用户不能更改密码)。这样就可以让那些企图入侵的黑客们花费一番工夫，并且可以借此发现他们的入侵企图。

具体做法如下：

依次单击“开始”→“设置”→“控制面板”，然后依次双击“管理工具”→“计算机管理”。

在弹出的窗口中单击“本地用户和组”前面的“+”，然后单击“用户”，在右边出现的用户列表中单击右键，在弹出的快捷菜单中单击“新用户”命令，在稍后弹出的“新用户”对话框中，输入用户名和一个足够复杂的密码，并选中“用户不能更改密码”复选框，如图6.6所示。

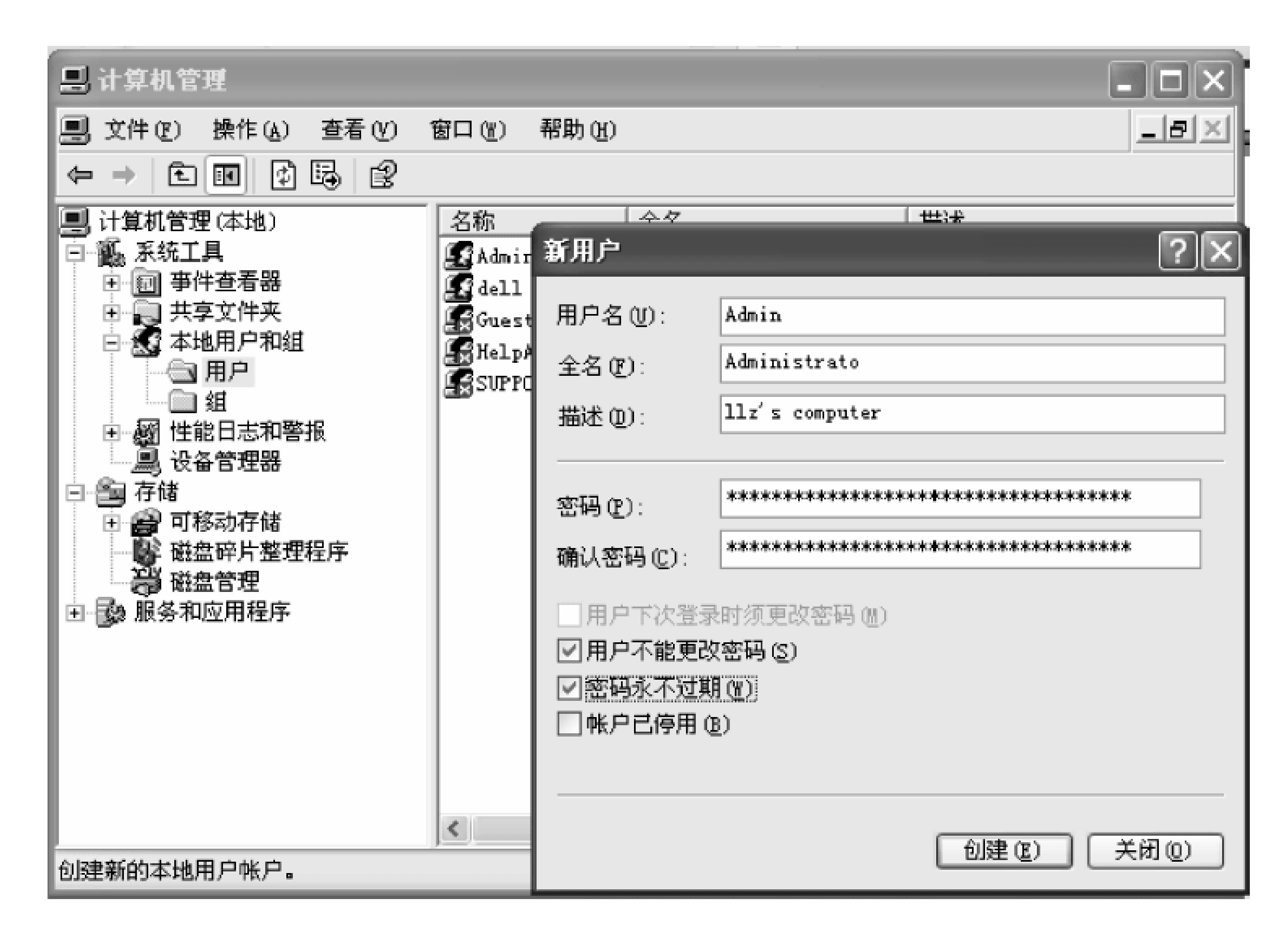


图 6.6 创建 Admin 新用户

单击“创建”按钮后，会发现在用户列表中已经出现了Admin账户，如图6.7所示。

将新创建的Admin用户添加到Guests组中，即单击“计算机管理”的“系统工具”中的“本地用户和组”前面的“+”，然后单击“组”，在右边出现的用户列表中单击右键，在弹出的快捷菜单中单击“添加到组”命令，如图6.8所示。



图 6.7 Admin 账户已创建

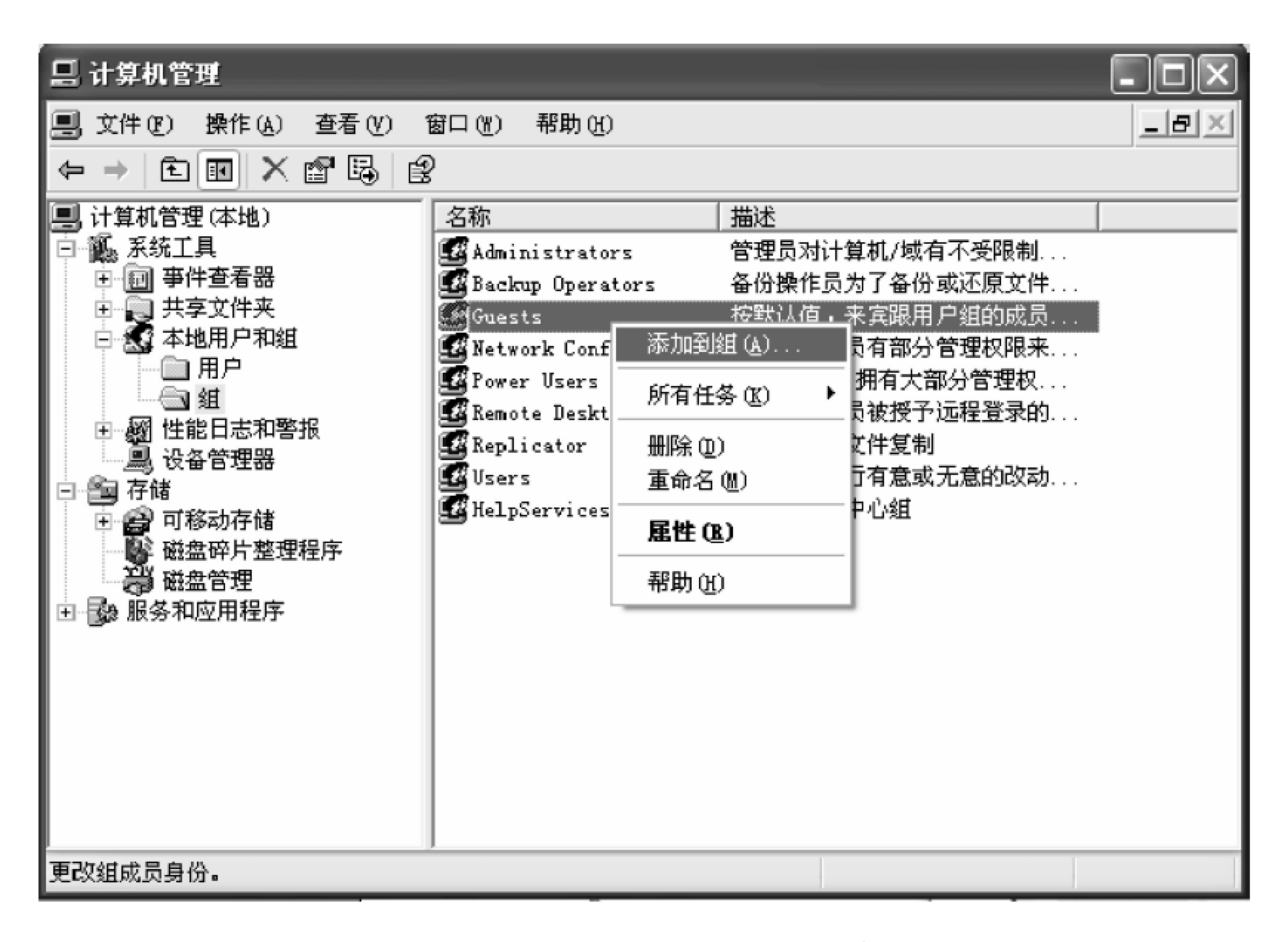


图 6.8 向 Guests 组添加新用户

在弹出的“选择用户”对话框中单击“高级”按钮，如图 6.9 所示。

在弹出的“高级”对话框中单击“立即查找”，在查找到的用户列表中选中 Admin，如图 6.10 所示。然后单击“确定”按钮，出现图 6.11 的 Guests 对话框，由此可见 Admin 账户已经添加到 Guests 组中了。





图 6.9 “选择用户”对话框



图 6.10 “选择用户-高级”对话框



图 6.11 Guests 组中已添加 Admin 账户

6.5.2 本地安全策略设置

1. 利用密码策略强制设置高强度密码

打开“本地安全设置”窗口，在窗口左边部分依次选择“账户策略”→“密码策略”，如图 6.12 所示。

然后在窗口右侧列出的策略中双击“密码必须符合复杂性要求”，在“密码必须符合复杂性要求 属性”对话框中选中“已启用”，单击“确定”按钮，如图 6.13 所示。

注：当启用“密码必须符合复杂性要求”策略后，密码必须符合下列要求才有效。

(1) 不得明显包含用户账户名或用户全名的一部分。

(2) 长度至少为 6 个字符。

(3) 包含来自以下 4 个类别中的 3 种字符：

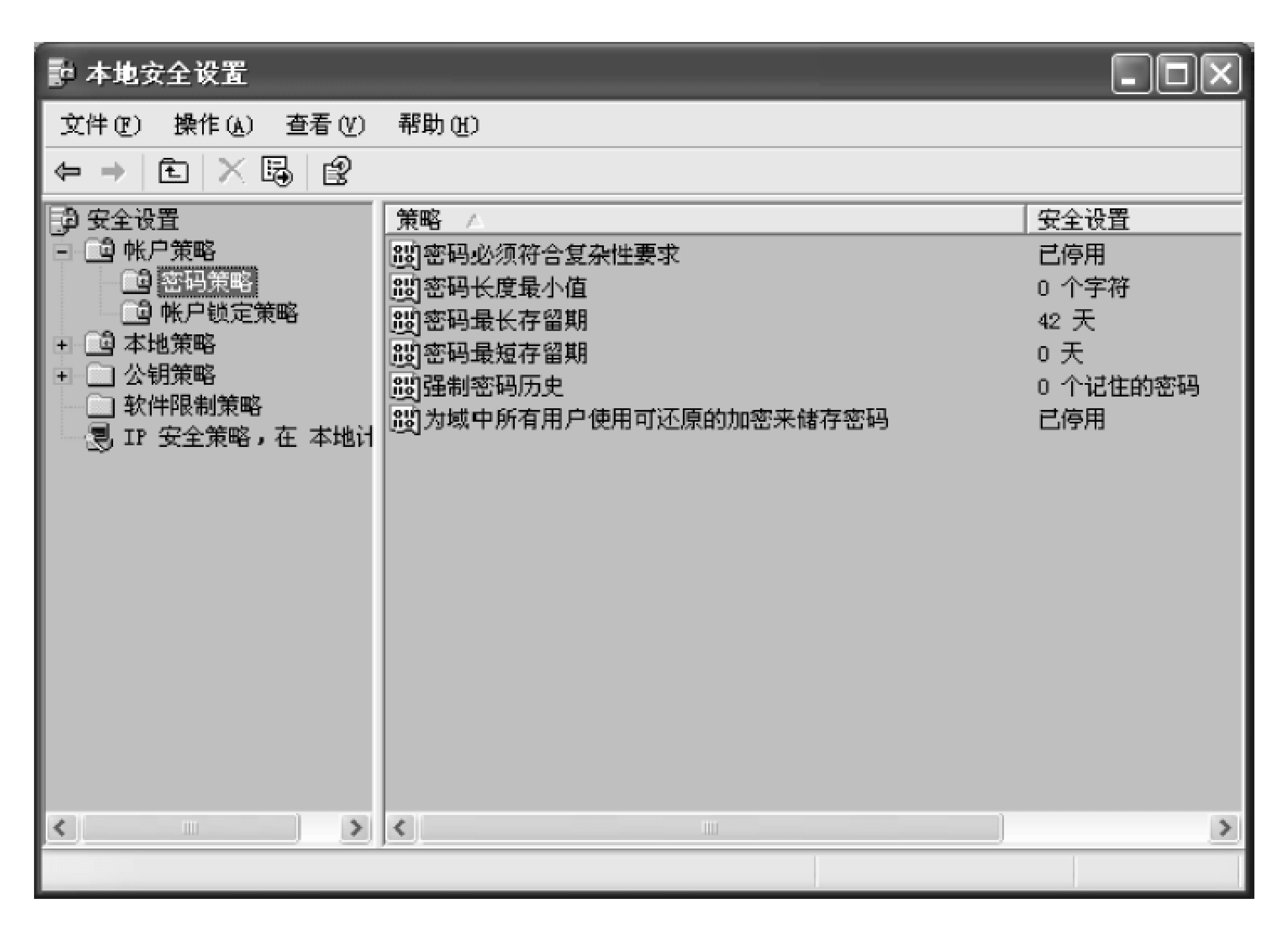


图 6.12 选择“密码策略”

• 英文大写字母(从 A 到 Z)；
• 英文小写字母(从 a 到 z)；
• 10 个基本数字(从 0 到 9)；
• 非字母字符(例如，!、$、#、%)。



图 6.13 设置密码复杂性策略

依次选择“控制面板”→“管理工具”→“计算机管理”，在“计算机管理”窗口的左侧部分依次选择“系统工具”→“本地用户和组”→“用户”，然后在窗口右侧右键单击 Administrator 账户，在弹出的快捷菜单中选择“设置密码”，如图 6.14 所示。

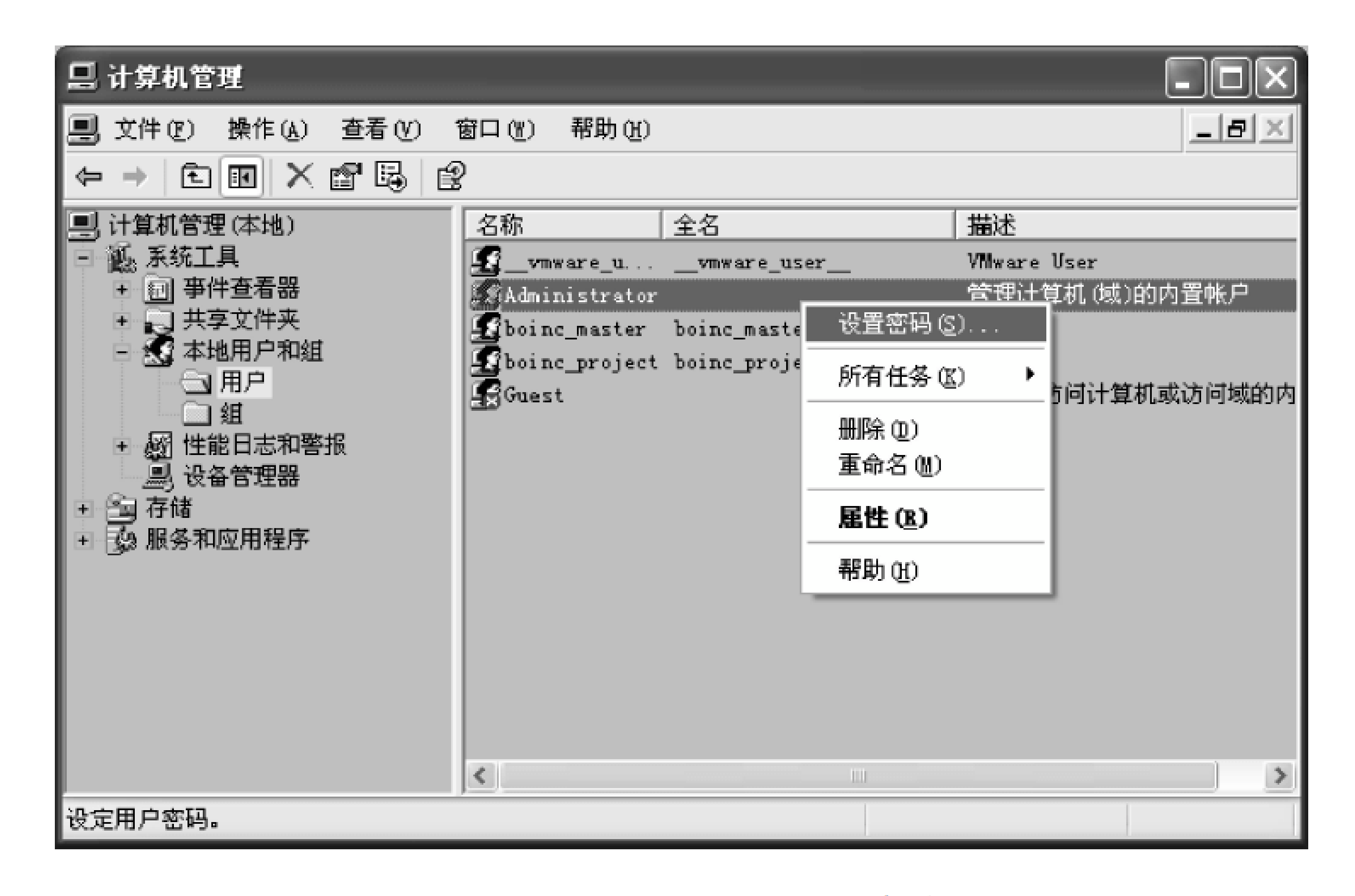


图 6.14 设置 Administrator 账户的密码

此时在弹出“为 Administrator 设置密码”对话框中，输入 123456，因为已经启用“密码必须符合复杂性要求”安全策略，所以若设置简单密码，则会弹出如图 6.15 所示的提示。



图 6.15　提示密码设置不符合要求

2. 保护密码安全策略的设置

(1) 设置密码长度最小值

设置密码长度最小值有助于防止用户设置过短的密码，避免用户密码被轻易猜出。

打开“本地安全策略”，在窗口右侧双击“密码长度最小值”，则打开了该项策略的设置，如图 6.16 所示。



图 6.16　设置密码长度最小值

一旦该策略生效，再次更改密码时，则必须符合该策略中设置的密码长度，否则会弹出与图 6.15类似的错误提示。

(2) 密码最长存留期与密码最短存留期

设置密码最长存留期可提醒用户在经过一定时间后更改正在使用的密码，这有助于防止长时间使用固定密码带来的安全隐患。设置密码最短存留期不仅可避免由于高度频繁地更改密码带来的密码难以使用的问题(如由于高度频繁地更改密码导致用户记忆混乱)，而且可防止黑客在入侵系统后更改用户密码。

打开“本地安全策略”，在窗口右侧双击“密码最长存留期”，则打开了该项策略的设置，如图 6.17 所示(以类似的方式，可以进行“密码最短存留期”的设置)。

(3) 强制密码历史

“强制密码历史”安全策略可有效防止用户交替使用几个有限的密码所带来的安全问

题。该策略可以让系统记住用户曾经使用过的密码。若用户更改的新密码与已使用过的密码一样，系统会给出提示。该安全策略最多可以记住 24 个曾使用过的密码。

打开“本地安全策略”，在窗口右侧双击“强制密码历史”，则打开了该项策略的设置，如图 6.18 所示。




图 6.17 设置密码最长存留期



图 6.18 设置强制密码历史

注：为了使“强制密码历史”安全策略生效，必须将“密码最短存留期”的值设为一个大于 0 的值。

(4) 账户锁定策略

账户锁定策略可发现账户操作中的异常事件，并对发生异常的账户进行锁定，从而保护账户的安全性。

打开“本地安全策略”窗口，在窗口左侧依次选择“账户策略”→“账户锁定策略”，则会看到该策略有 3 个设置项：“复位账户锁定计数器”、“账户锁定时间”、“账户锁定阈值”，如图 6.19 所示。



图 6.19 账户锁定策略

“账户锁定阈值”可设置在几次登录失败后就锁定该账户。这能有效防止黑客对该账户密码的穷举猜测。当“账户锁定阈值”的值设定为一个非0值后，则可以设置“复位账户锁定计数器”和“账户锁定时间”两个安全策略的值。其中“复位账户锁定计数器”设置了计数器复位为0时所经过的分钟数；“账户锁定时间”设置了账户保持锁定状态的分钟数，当时间过后，账户会自动解锁，以确保合法的用户在账户解锁后可以通过使用正确的密码登录系统。

当“账户锁定阈值”设置为一个非0值后，“复位账户锁定计时器”与“账户锁定时间”会自动设置为默认值，如图6.20所示。默认值可在这两个安全策略中分别修改。

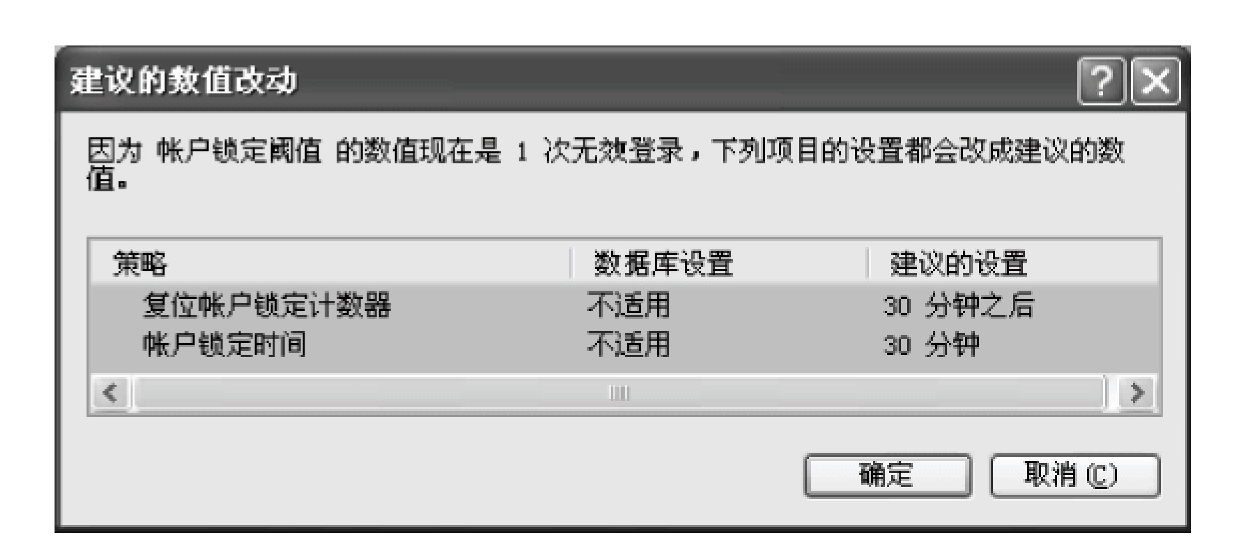


图6.20 “复位账户锁定计数器”与“账户锁定时间”的默认值

6.5.3 利用SYSKEY保护账户信息

SYSKEY可以使用启动密钥来保护SAM文件中的账户信息。默认情况下，启动密钥是一个随机生成的密钥，存储在本地计算机上。这个启动密钥在计算机启动时必须正确输入才能登录系统。运行SYSKEY有两种方式：

1. 依次单击“开始”→“运行”命令，在“运行”对话框中输入syskey命令，如图6.21所示。然后单击“确定”按钮，会出现如图4.22所示的SYSKEY设置界面。



图6.21 运行SYSKEY

2. 依次单击“开始”→“程序”→“附件”→“命令提示符”命令，在盘符后输入syskey命令，按Enter键，会出现“保证Windows XP账户数据库的安全”的对话框，也就是SYSKEY的设置界面，如图6.22所示。单击“确定”按钮，此刻会发现操作系统没有任何提示，但是其实已经完成了对SAM散列值的二次加密工作。此时，即使攻击者通过另外一个系统进入硬盘，盗走SAM文件的副本或者在线提取密码散列值，这份副本或散列值对于攻击者也是没有意义的，因为SYSKEY提供了安全保护。

如果要设置系统启动密码或启动软盘就要单击对话框中的“更新”按钮，弹出如图6.23所示的对话框。

- 若想设置系统启动时的密码可以单击“密码启动”，并在文本框中输入你设置的密码。
- 若想制作启动软盘可以依次单击“系统产生的密码”和“在软盘上保存启动密码”。
- 若想保存一个密码作为操作系统的一部分，在系统开始时不需要任何交互操作，可依次单击“系统产生的密码”和“在本机上保存启动密码”。



图 6.22 启用 SYSKEY

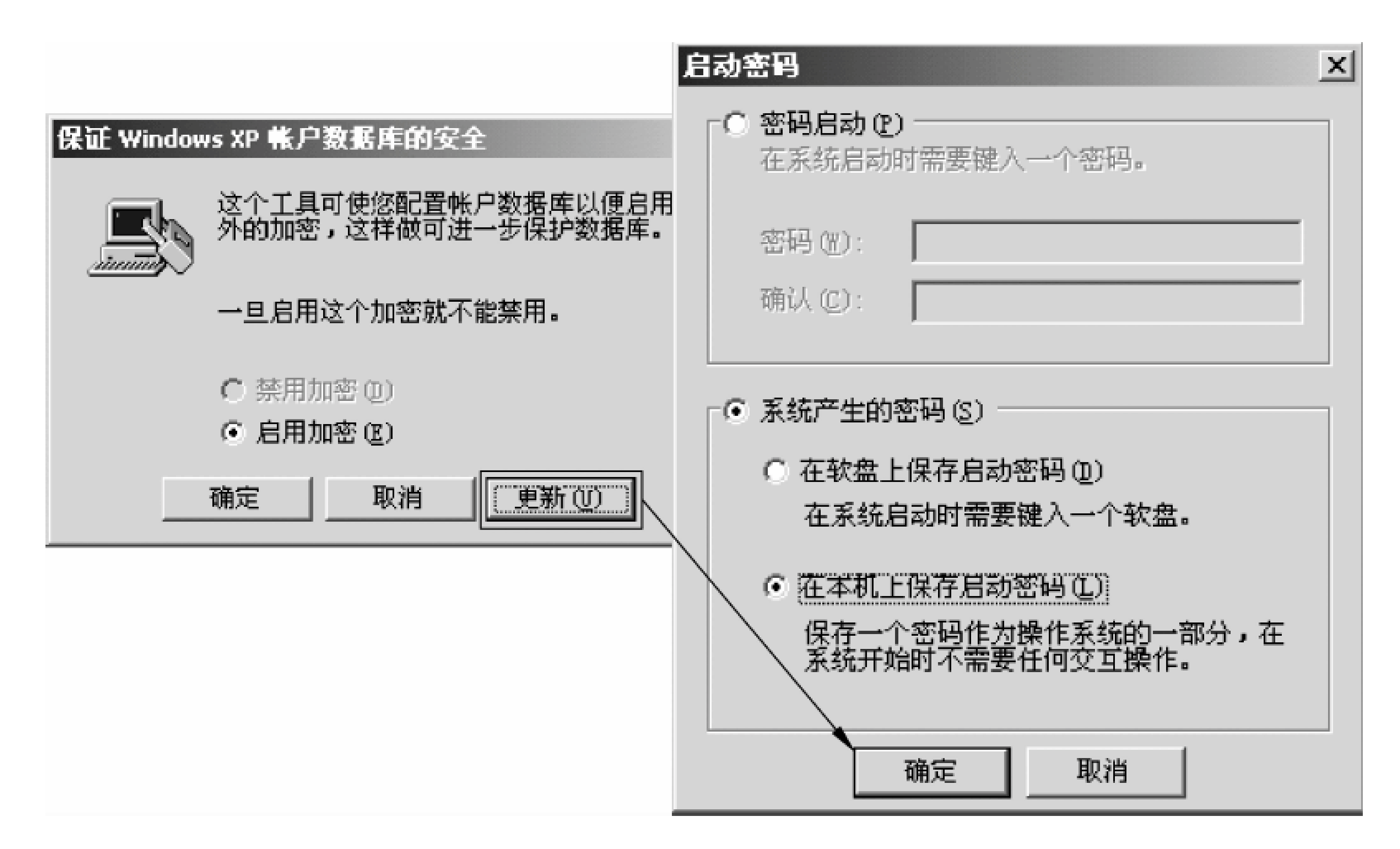


图 6.23 启动密码设置

当然，要防止黑客进入系统后对本地计算机上存储的启动密钥进行暴力搜索，还是建议将启动密钥存储在软盘或移动磁盘上，实现启动密钥与本地计算机的分离。

6.6 实验思考

（1）在密码策略中将密码的最小长度设置为7，然后在命令行中利用 net user 命令创建一个 test 账户，并将其密码设置为123456，观察会出现何种提示信息。

（2）将"账户锁定阈值"设置为1，将"复位账户锁定计数器"和"账户锁定时间"保留为系统默认值，然后故意让某个账户进行1次失败登录，观察经过多长时间后，该账户才能正常地登录系统。

实验7 EFS 实验

7.1 实验目的与要求

- 掌握 EFS 的概念及原理。
- 掌握如何使用 EFS 加密文件以及文件夹。
- 掌握如何设置 EFS 的加密文件恢复代理。

7.2 实验环境

Windows XP 操作系统。

7.3 预备知识

EFS(Encrypting File System,加密文件系统)是 Windows 2000 以上系统中 NTFS 分区下提供的一种透明的文件加密功能,即使用户对于加密机制一无所知,也能对存储在硬盘上的文件夹或者单个文件进行加解密,以防止系统的非法入侵者对敏感数据的访问,而对于合法的授权用户而言,访问加密文件与访问普通文件表面上并无区别。

EFS 具有以下特点。

(1) EFS 基于 PKI(Public Key Infrastructure,公钥基础设施)技术以及 CryptoAPI 架构,采用公钥密码体制与对称钥密码体制相结合的方式来对文件和文件夹进行加密,不仅能够实现加密的高效率,而且能够保证文件加密密钥的安全。

(2) 访问加密文件非常方便,任何合法的授权用户均可以像访问普通文件一样去访问加密文件,而不需要在每次读取加密文件时输入密码。

(3) 加密后的数据在改变存储位置时(在 NTFS 分区下的移动)会保持加密状态。当把一个文件复制到一个加密的文件目录中时,该文件也会被加密。当试图将加密后的文件从 NTFS 分区移动到非 NTFS 分区时会遭到拒绝。

(4) EFS 与 NTFS 紧密结合。当访问一个加密文件时,用户首先需要具有访问该文件的 NTFS 权限,此时用户能够看到该加密文件。如果

要读取该文件,那么用户还需要具有该加密文件对应的私钥。

(5) EFS 可提供数据恢复代理的功能,被指定为数据恢复代理的账户可以恢复别的用户加密的文件或者文件夹。在 Windows 2000 中,内置管理员账号被指定为默认的数据恢复代理;在 Windows XP 以后的版本中,未设置默认的数据恢复代理,但是可以通过手工添加一个代理。

一旦用户通过操作系统发出一个加密命令,EFS 将按照如下流程去工作。

(1) EFS 首先进行一系列的检查,这些检查包括文件或文件夹能否被加密,比如当前用户是否有加密权限、文件是否是系统文件(系统文件或在系统目录中的文件不能被 EFS 加密)或者是否有足够的磁盘空间来实施加密。如果经过检查后文件可以被加密,EFS 则通过 CryptoAPI 接口调用 Microsoft Base Cryptographic Provider 1.0 来产生 FEK(File Encryption Key,文件加密密钥)。

(2) 检查当前登录操作系统的用户是否拥有一个包含私钥的 X.509 数字证书。如果没有,EFS 则自动为当前用户产生一个此类证书。然后,EFS 将使用该证书中的公钥去加密 FEK。

(3) EFS 为当前用户创建两个数据块:DDF(数据解密块)和 DRF(数据恢复块)。如果存在多个授权用户可访问加密文件,EFS 会使用这些授权用户的公钥分别去加密 FEK,并产生一个 FEK 列表。该 FEK 列表与使用 FEK 加密后的文件会被一起存储在 DDF 中。如果系统设置了一个或者多个数据恢复代理,那么 FEK 还会被数据恢复代理的公钥加密,然后形成一个 FEK 列表并与加密后的文件一起存储到 DRF 中(由于只有当 FEK 被数据恢复代理的公钥加密后,数据恢复代理才能使用私钥解密 FEK,进而解密 FEK 加密的文件,因此对于数据恢复代理之前的加密文件,由于其 FEK 没有被数据恢复代理的公钥加密,数据恢复代理则不能解密这些文件)。

(4) 为防止加密过程中出现严重错误,进而导致文件无法被恢复,加密文件时 EFS 将在文件所在的文件夹中创建一个名为 efs0.tmp 的临时文件,首先将要加密的文件内容复制到该临时文件中,然后原文件内容被加密的数据覆盖。

(5) 将第(4)步中创建的临时文件 efs0.tmp 删除。

加密的过程如图 7.1 所示。

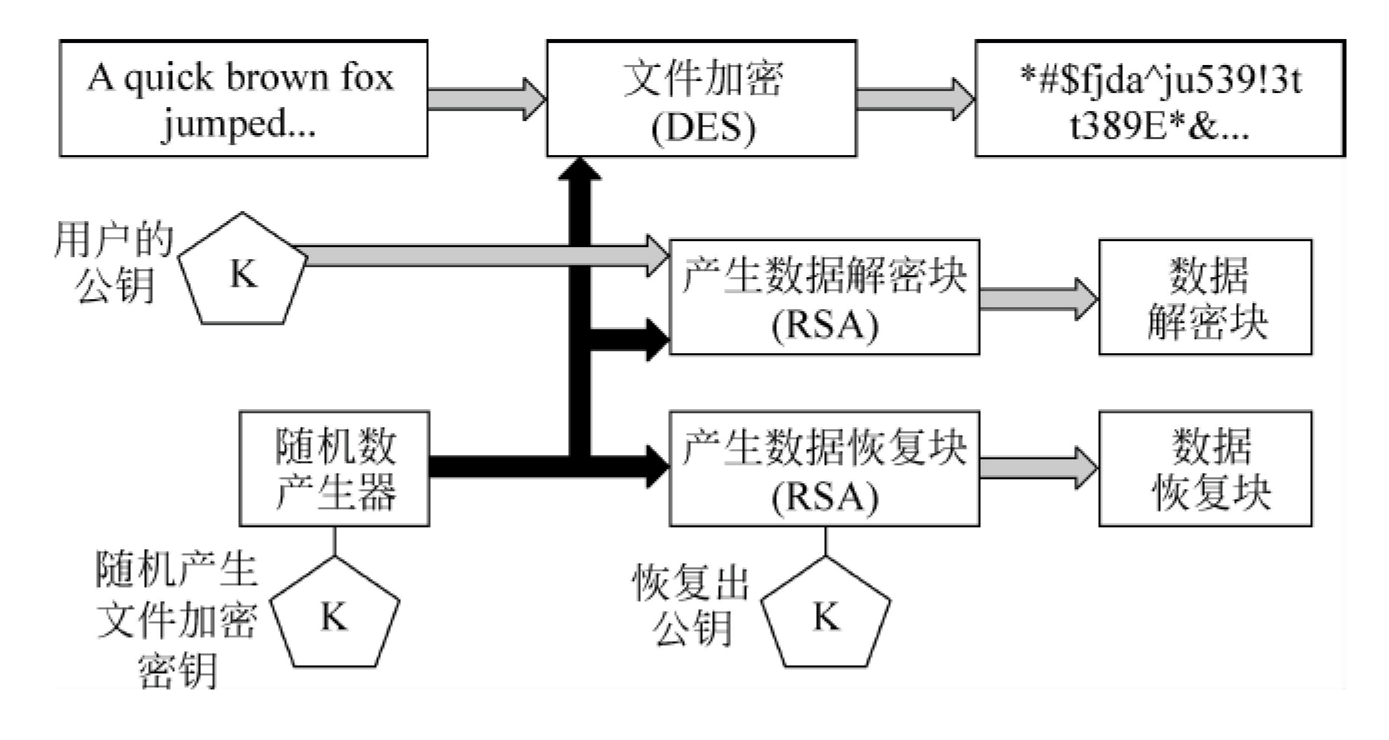


图 7.1 EFS 的加密过程

解密过程与加密过程是相反的，如图 7.2 所示。

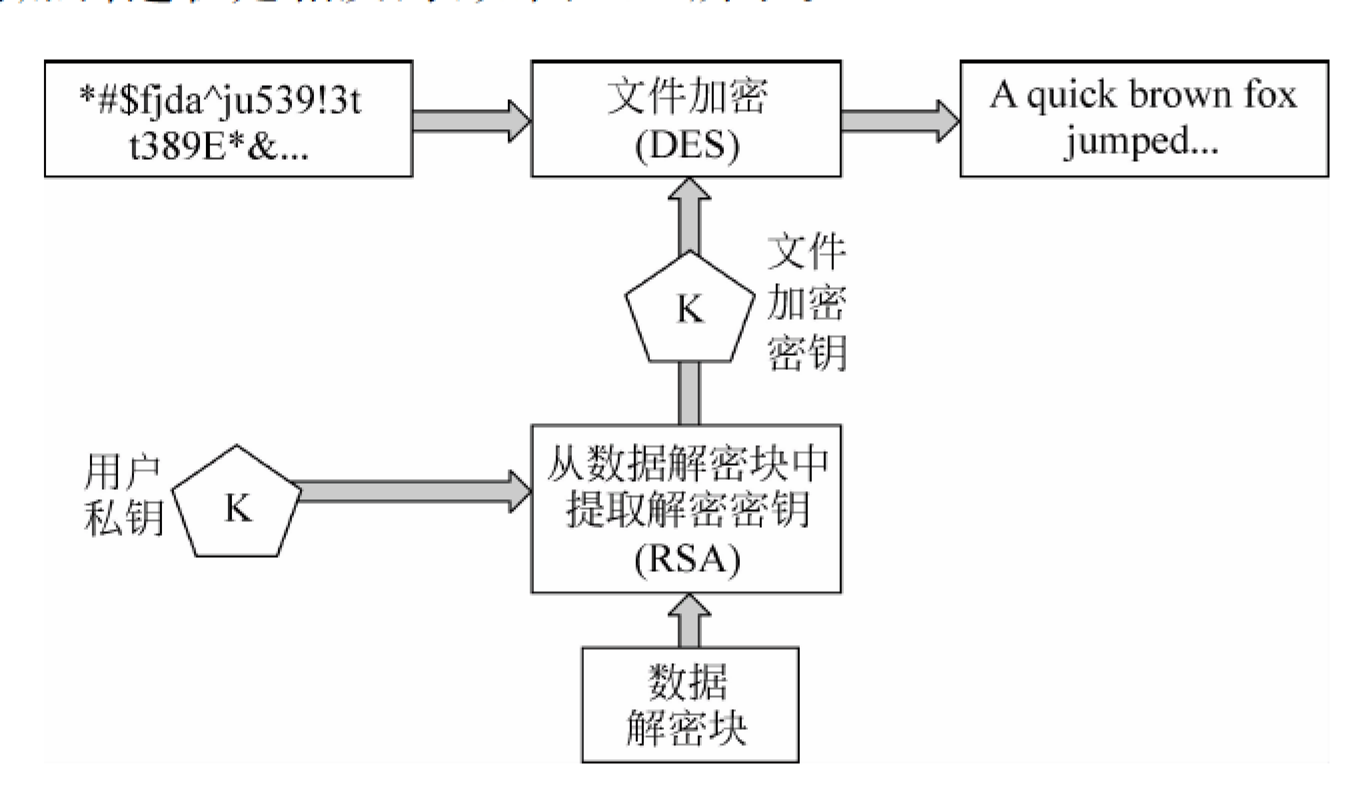


图 7.2　EFS 的解密过程

在解密过程中，系统首先判断当前用户是否具有访问加密文件的 NTFS 权限，若具有该权限，那么再判断当前用户是否具有加密 FEK 的公钥所对应的私钥。若具有该私钥，那么 EFS 将在 DDF 和 DRF 队列中寻找当前用户的 DDF 或者 DRF，找到后，则使用用户自己的私钥解密出 FEK，然后用 FEK 去解密加密文件。

7.4　实验内容

本章的实验内容主要包括以下 3 部分：

(1) 演示如何在 Windows 系统的 NTFS 文件系统下对文件实施加密。

(2) 通过数字证书的导入和导出来演示 EFS 加密的原理，即文件加密是基于数字证书中的密钥完成的。

(3) 演示数据恢复代理的使用方法。

7.5　实验步骤

7.5.1　利用 EFS 加密文件

首先在操作系统上创建两个账户分别为 EFS_User 和 EFS_User1，并首先以 EFS_User 账户进入操作系统。

打开桌面上的"我的电脑"，在"我的电脑"窗口上方的主菜单中依次单击"工具"→"文件夹选项"，打开"文件夹选项"对话框。在该对话框中选择"查看"选项卡，并在"高级设置"栏下的"用彩色显示加密或压缩的 NTFS 文件"复选框中打钩，如图 7.3 所示。

在一个 NTFS 分区上创建一个文本文件 paper.txt，并输入内容，如图 7.4 所示。

右键单击 paper.txt，在弹出的快捷菜单中选择"属性"，打开 paper.txt 的"属性"对话框。

选择"属性"对话框的"常规"选项卡，单击下方的"高级"按钮，打开"高级属性"对话框。在"压缩或加密属性"栏下的"加密内容以便保护数据"复选框前打钩，然后单击"确定"按钮，如图 7.5 所示。此时会发现文件 paper.txt 的文件名变为绿色，这说明该文件已被加密。

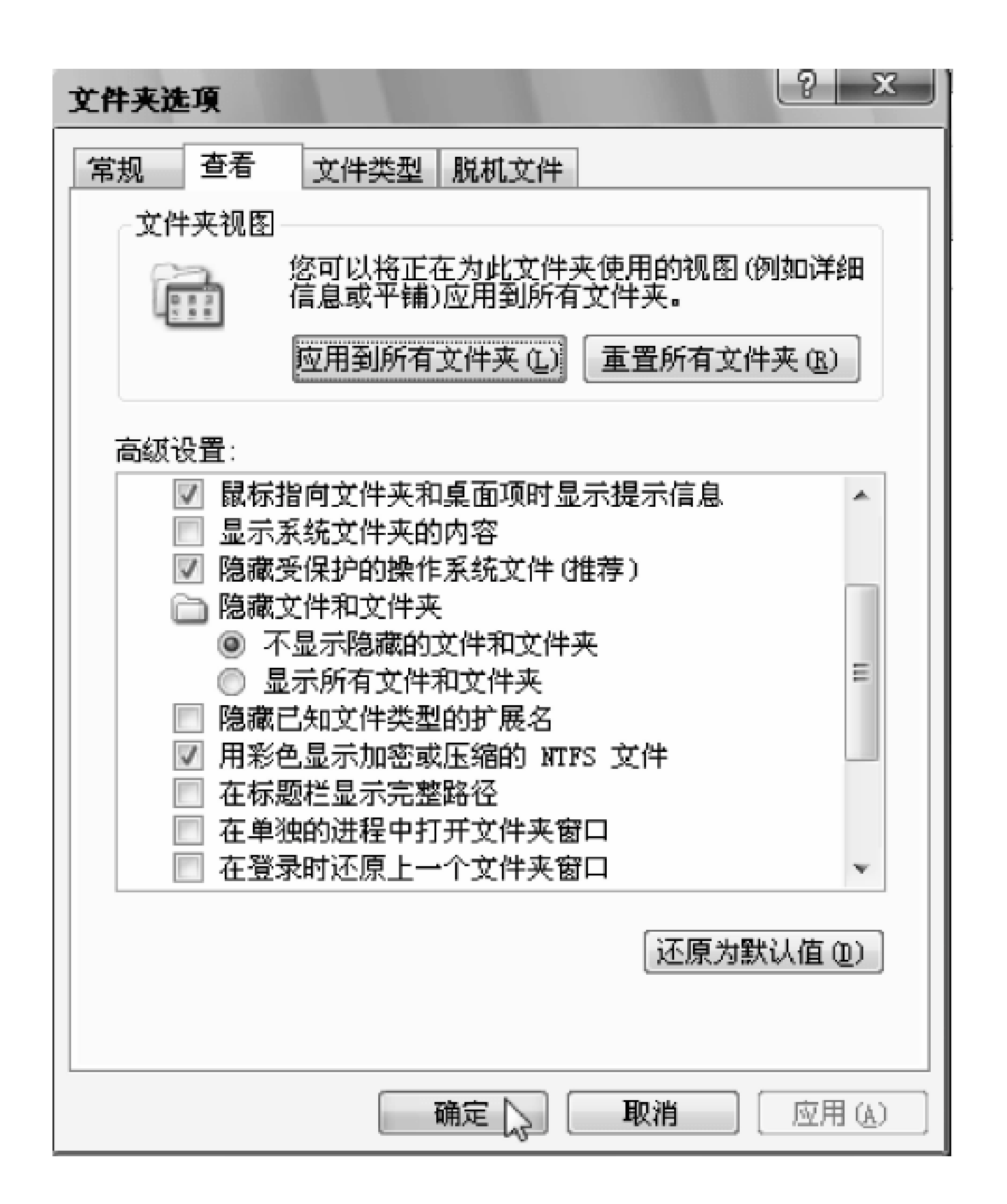


图 7.3 文件夹选项



图 7.4 创建 paper. txt 文件



图 7.5 加密文件

依次单击“开始”→“运行”命令，打开“运行”对话框，输入 certmgr.msc 命令（Windows 系统自带的数字证书管理工具），单击“确定”按钮，打开“证书”对话框，在个人证书分支树下会出现一个“颁发给”信息和“颁发者”信息均为“EFS_User”的证书，如图 7.6 所示。

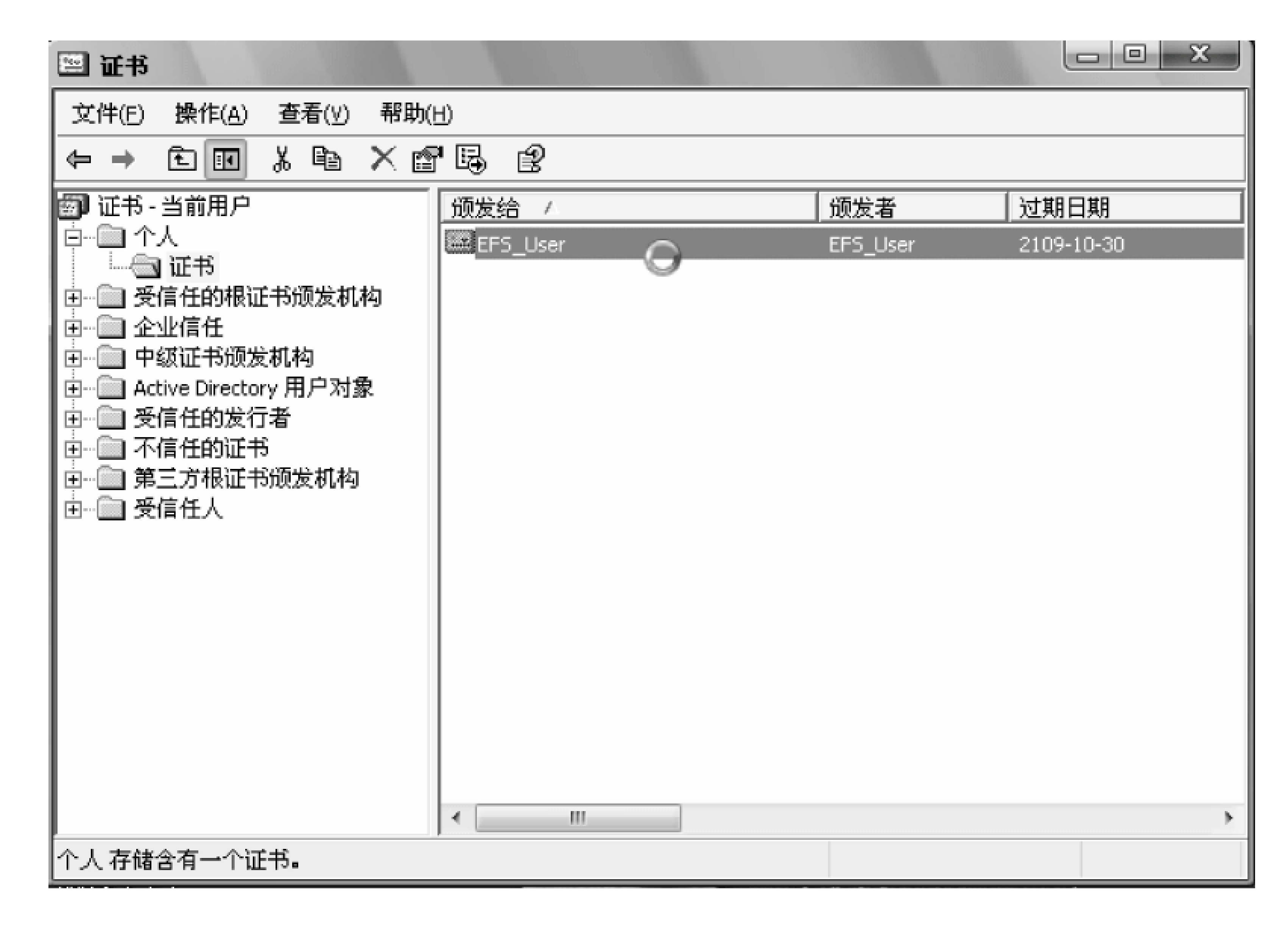


图 7.6 EFS_User 的证书管理器

双击该证书，则显示该证书的详细信息，其中提示该证书含有一个私钥，如图 7.7 所示。使用该私钥，用户 EFS_User 可以解密出加密文件 paper.txt 的密钥 FEK，然后使用 FEK 便可以解密文件 paper.txt。

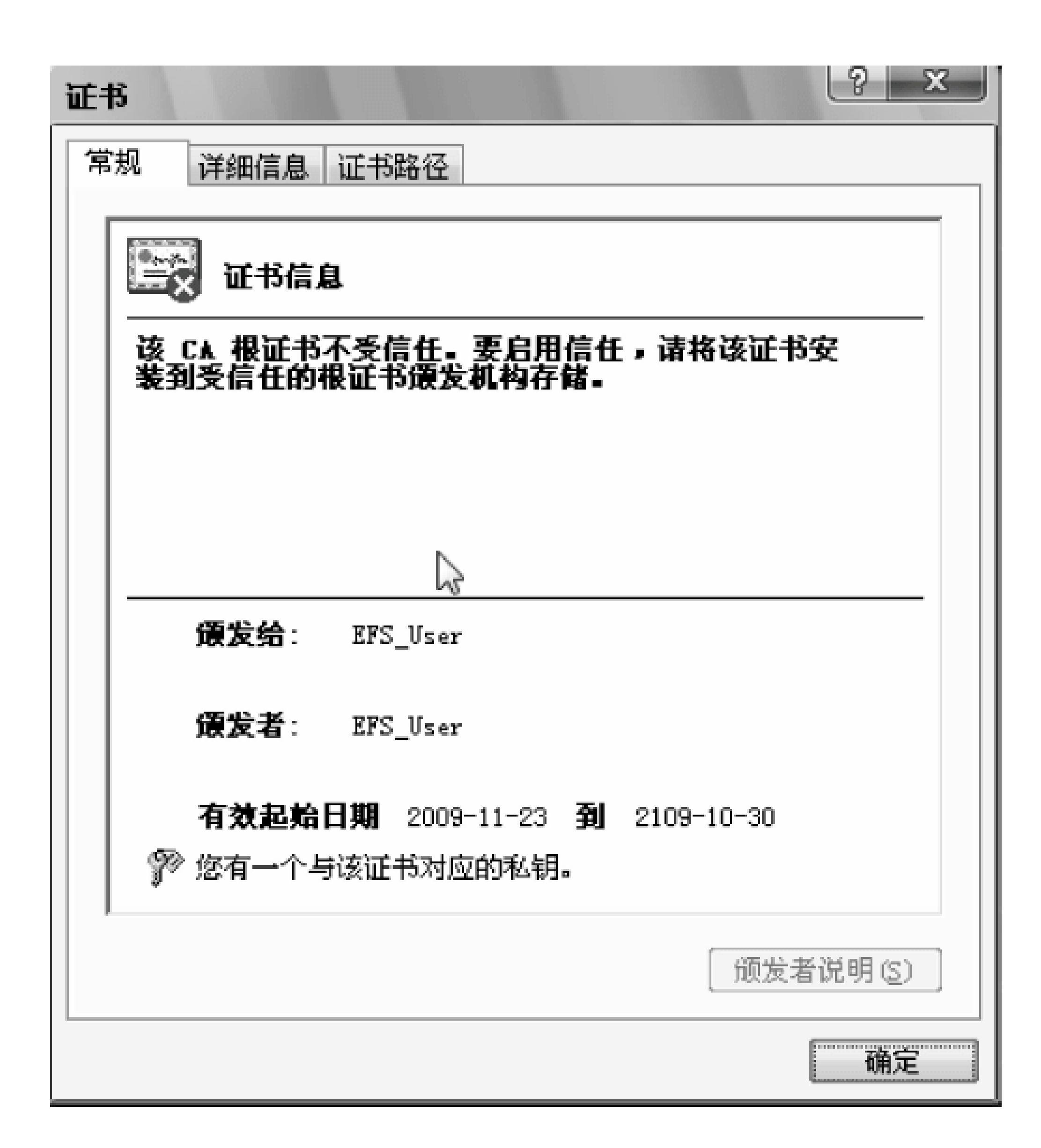


图 7.7 用于加解密的数字证书

注：加密文件 paper.txt 的文件密钥 FEK 是用该证书的公钥加密的。

7.5.2 证书的导出

在证书管理器中，右键单击 EFS_User 的证书，在弹出的快捷菜单中依次选择“所有任务”→“导出”，进入“证书导出向导”，如图 7.8 所示。



图 7.8　导出证书到文件中

在证书导出向导的第二步选择“是，导出私钥”，如图 7.9 所示，然后根据向导提示将该证书导出到一个名为 EFS_Use.pfx 的证书文件中。

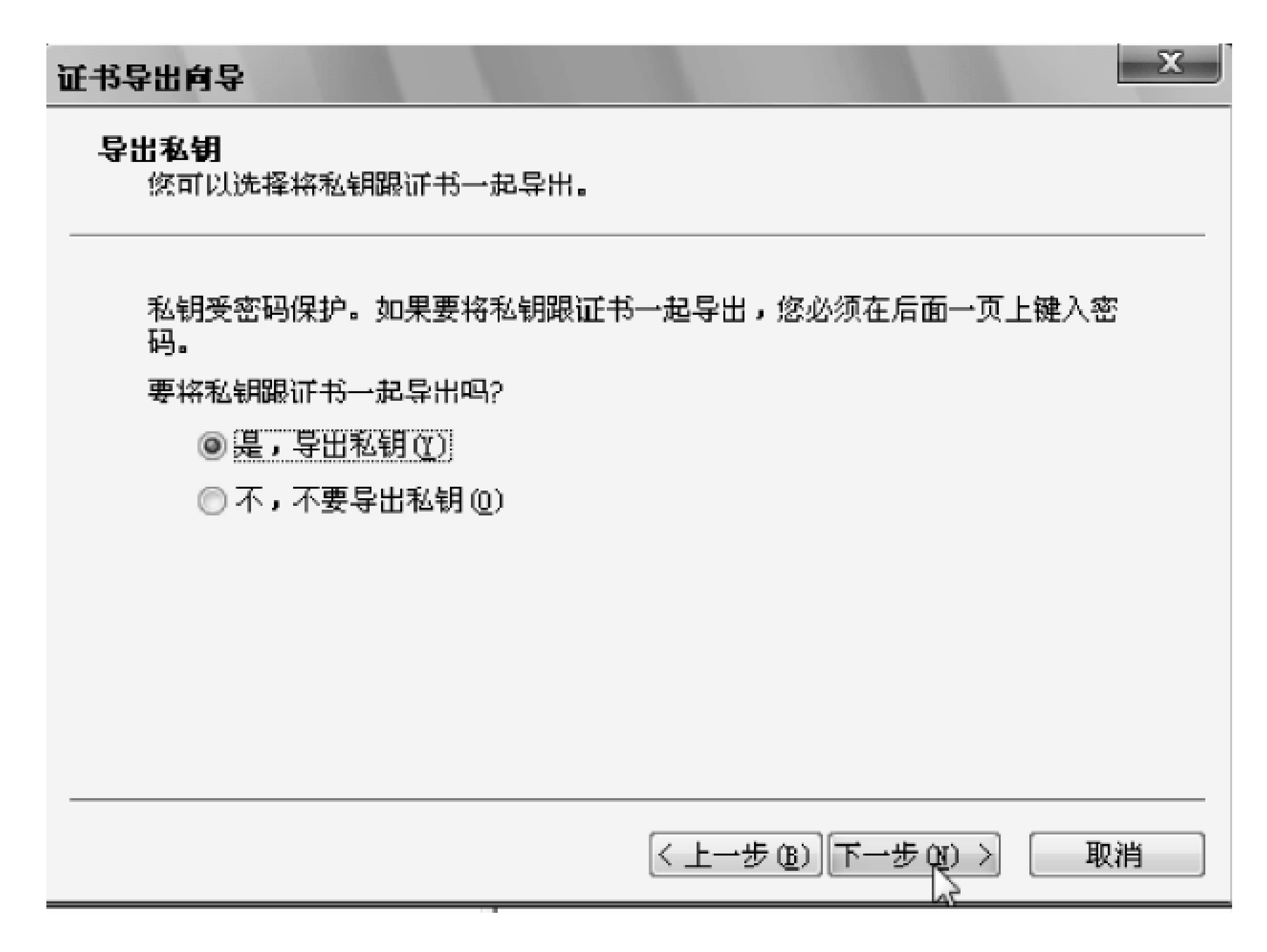


图 7.9　选择导出私钥

注销账户 EFS_User，然后以 EFS_User1 账户登录系统，并打开加密文件 paper. txt，会出现错误提示“拒绝访问”，如图 7.10 所示。

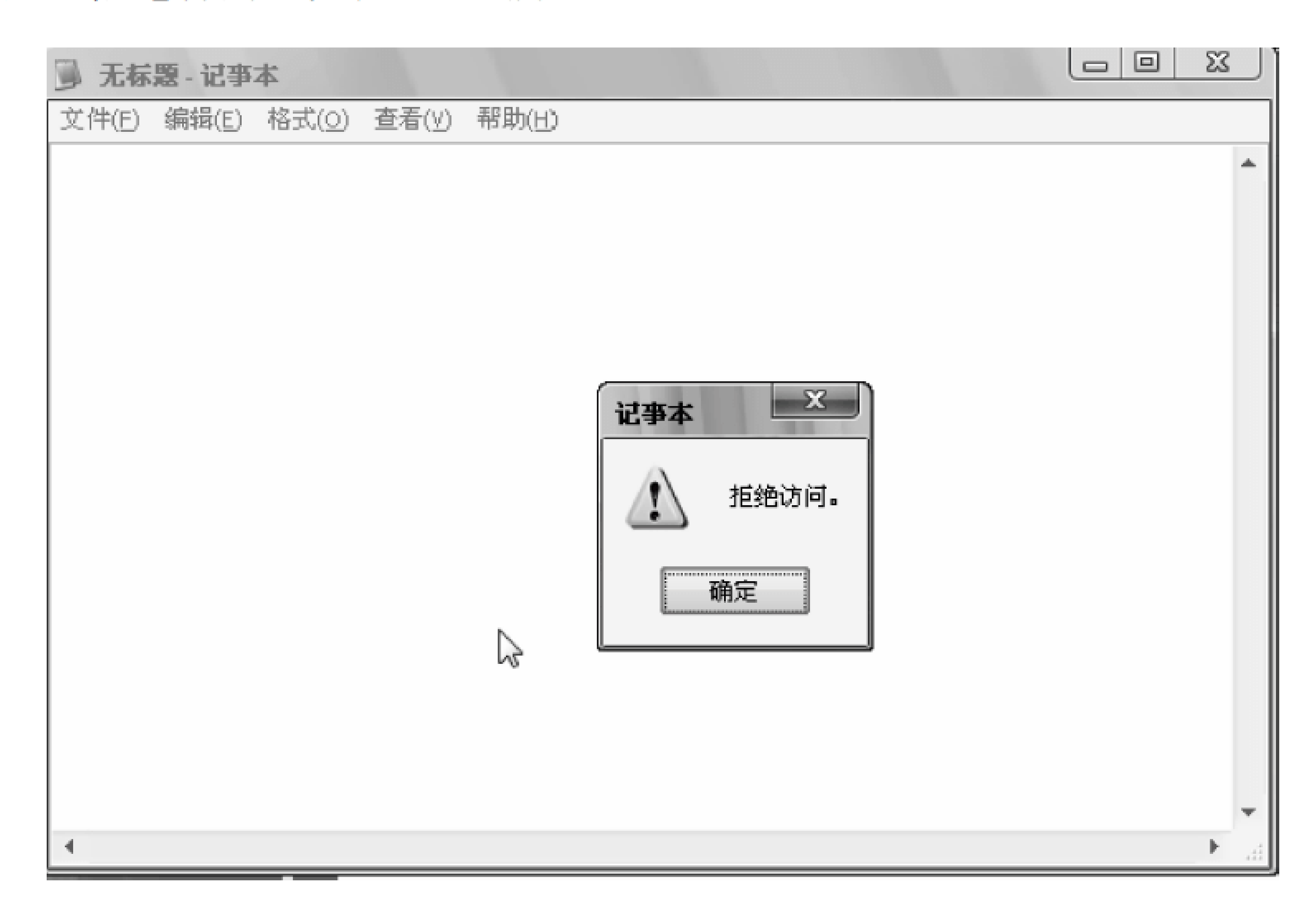


图 7.10 拒绝访问

在“运行”对话框中输入 certmgr. msc 命令，打开“证书”管理器，会发现在“个人”分支树下没有“颁发给”和“颁发者”信息均为“EFS_User”的数字证书，如图 7.11 所示。

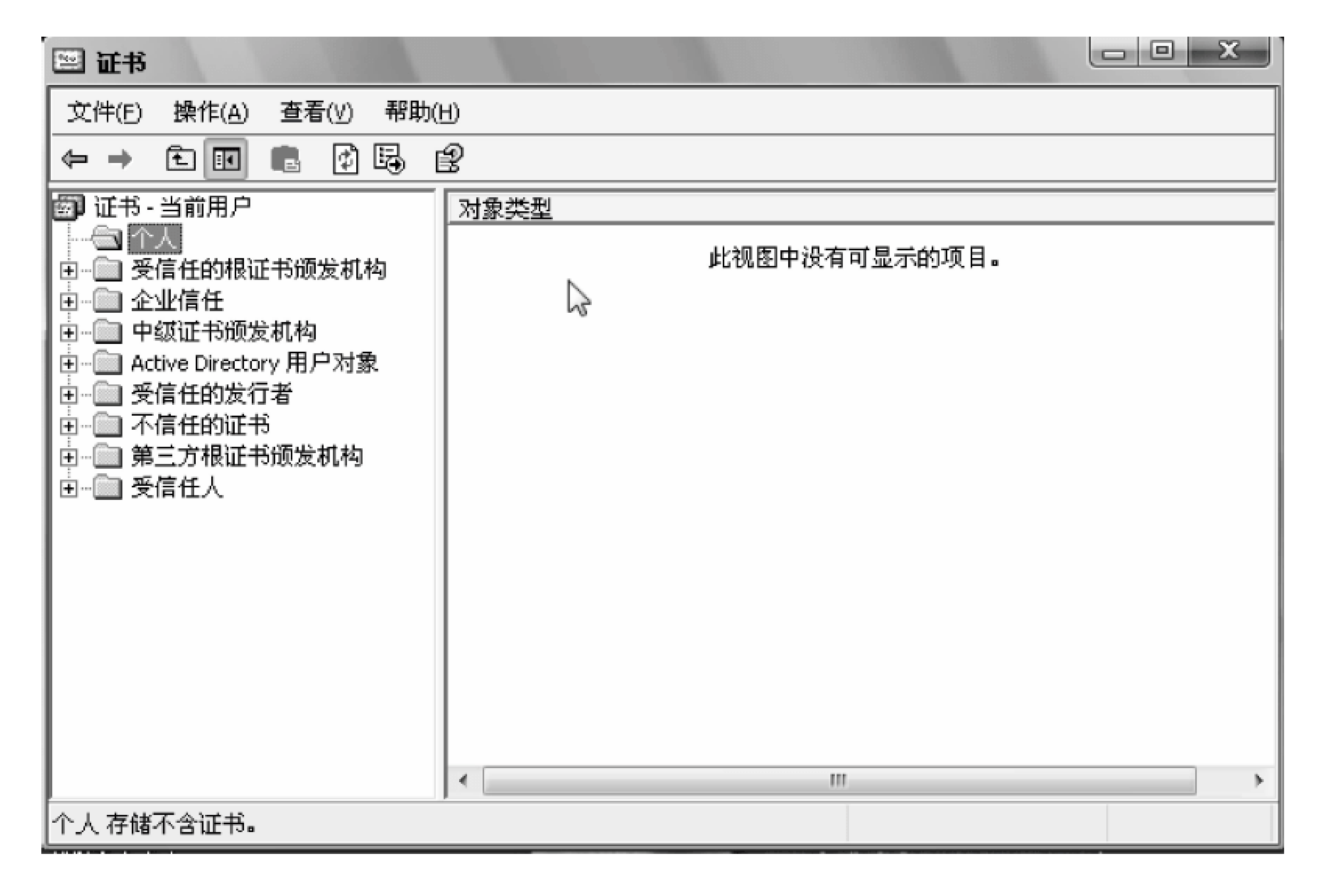


图 7.11 EFS_User1 的证书管理器

双击导出的名为 EFS_User. pfx 的证书文件，根据提示将该证书安装到证书管理器中(注：当前的账户是 EFS_User1)。

重新打开 paper. txt，会发现 paper. txt 可以打开。这说明只要具有 EFS_User. pfx，就可以打开 paper. txt 加密文件。

7.5.3 数据恢复代理

注销当前账户，并以 Administrator 账户登录系统。在“运行”对话框中输入 cmd 命令，单击“确定”按钮，进入控制台。

在命令提示符下输入 cipher /r：recovery，则会在当前目录下产生两个文件 recovery.cer 和 recovery.pfx，如图 7.12 所示。两者的区别在于前者仅包含证书，而后者除了包含证书外，还包含一个私钥。

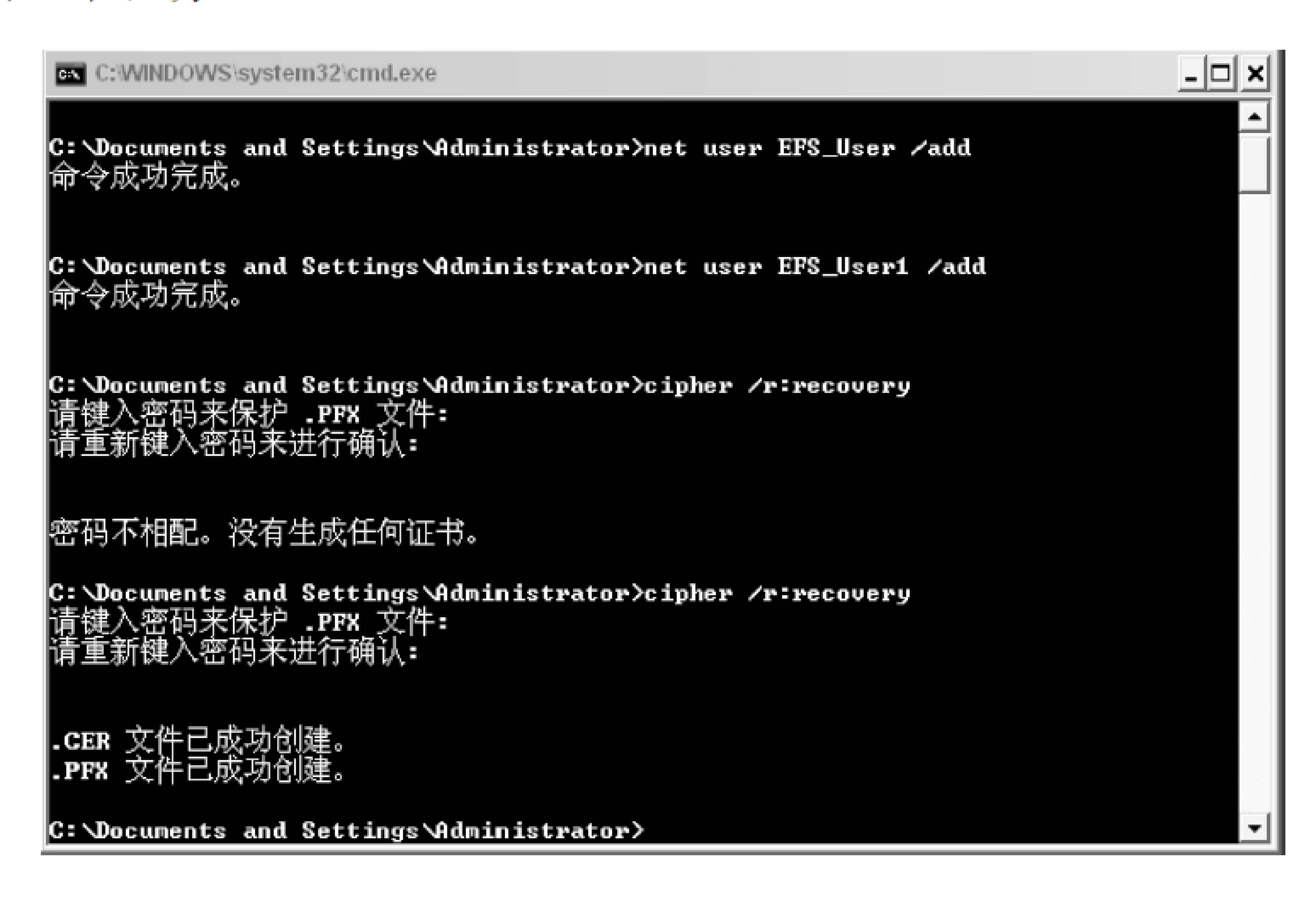


图 7.12 创建加密回复代理的证书文件

双击 recovery.pfx 数字证书文件，将该证书安装到“证书”管理器中。然后在“运行”对话框中输入 gpedit.msc 命令，单击“确定”按钮，进入“组策略”对话框。依次展开以下节点：计算机配置、Windows 设置、安全设置、公钥策略。右键单击“正在加密文件系统”，在弹出的快捷菜单中选择“添加数据恢复代理”，如图 7.13 所示，进入“添加故障恢复代理向导”。

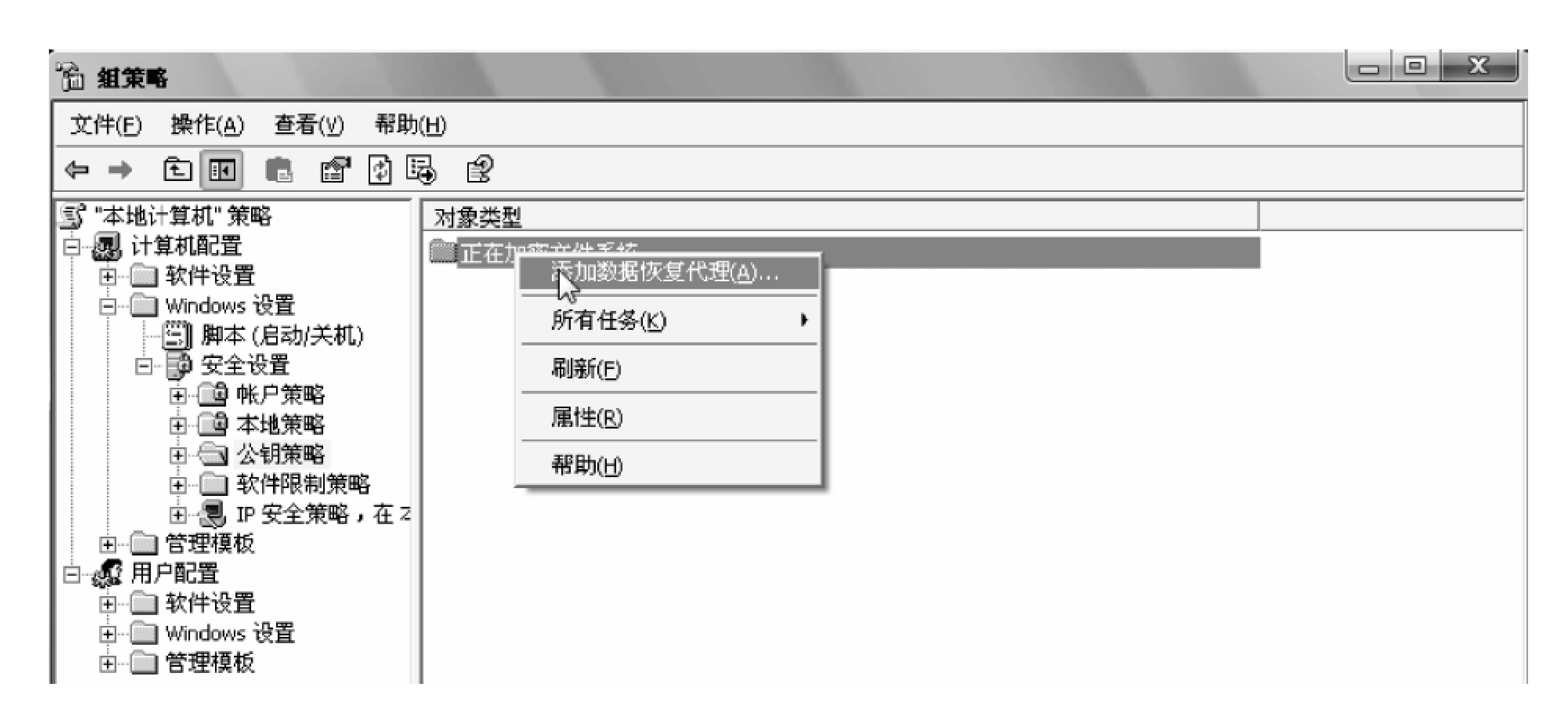


图 7.13 添加数据恢复代理

在该向导的第二步中，通过右侧的“浏览文件夹”按钮将产生的数字证书 recovery. cer 导入该向导，如图 7.14 所示。然后根据向导提示，完成数据恢复代理的添加(注：由于当前账户是 administrator，因此 administrator 为数据恢复代理)。



图 7.14　添加数据恢复代理向导

注销 Administrator 账户，以 EFS_User 登录系统，并创建另一个加密文件 paper1. txt。然后再以 Administrator 账户登录系统，此时可以打开加密文件 paper1. txt。然而在打开加密文件 paper. txt 时仍然会提示错误信息“拒绝访问”，这说明对于设置数据恢复代理之前加密的文件，数据恢复代理仍然是打不开的。

7.6　实验思考

(1) 请通过实验验证在 FAT 文件系统上能否实施 EFS 加密操作。

(2) 若在第 7.5.2 节中导出数字证书的过程中不导出私钥，那么在 EFS_User1 账户下导入不含私钥的数字证书后，能否解密 paper. txt？为什么？

实验8 FTP访问权限实验

8.1 实验目的与要求

- 理解 FTP 的概念及原理。
- 掌握 Windows 操作系统下 FTP 服务器的搭建方式。
- 掌握设置不同权限访问 FTP 服务器的方法。

8.2 实验环境

在 VMWare 虚拟机中安装 Windows 2003 Server 与 Windows XP 两种操作系统。Windows 2003 Server 作为服务器，IP 地址为 192.168.1.105，安装 FTP 服务；Windows XP 作为客户机，IP 地址为 192.168.1.102。

8.3 预备知识

FTP(File Transfer Protocol)是一种采用 TCP 协议的文件传输协议，使用该协议能够实现计算机之间大容量文件的快速传输。目前，FTP 是实现计算机网络(尤其是校园网)中文件共享的主要手段之一。FTP 采用 Client/Server(客户机/服务器)架构，用户在本地运行 FTP 客户端程序来使用 FTP 服务；远程服务器通过运行 FTP 服务器程序来提供 FTP 服务。从本地向远程服务器传输文件称为上载(upload)；将远程服务器中的文件传输到本地称为下载(download)。

为了满足众多用户的下载需求，FTP 提供匿名下载服务。当用户使用匿名下载服务时，可以使用“anonymous”作为用户名，并使用任何字符串作为密码(通常要求以用户的电子邮件地址作为密码，以便让站点的拥有者了解到哪些人在使用该服务)，连接到 FTP 服务器去下载所需文件。考虑到 FTP 服务器的安全，匿名账户仅拥有下载文件的权限，而不允许上传。为了方便 FTP 站点管理员的远程管理，可以在 FTP 站点上设置一个特殊权限的账户，管理员通过该账户登录到 FTP 站点上，能够上传文件，并对站点的内容进行管理。

FTP 支持两种工作方式：主动方式(Strandard 方式)与被动方式(Passive 方式)。主动方式下，FTP 客户机发送 Port 命令到 FTP 服务



器；被动方式下，FTP 客户机发送 Pasv 命令到 FTP 服务器。

1. 主动方式的工作原理

客户机上的 FTP 客户端软件打开客户机的一个大于 1024 的端口，并连接到 FTP 服务器的 21 端口，也就是命令端口。当客户机需要接收数据时，则向服务器的 21 端口发送 Port 命令，Port 命令中指明了客户机正在使用哪个端口接收数据。当 FTP 服务器需要向客户机传送数据时，则打开 20 端口连接至客户机的指定端口，并使用该连接传送数据给客户机。其连接过程如图 8.1 所示。

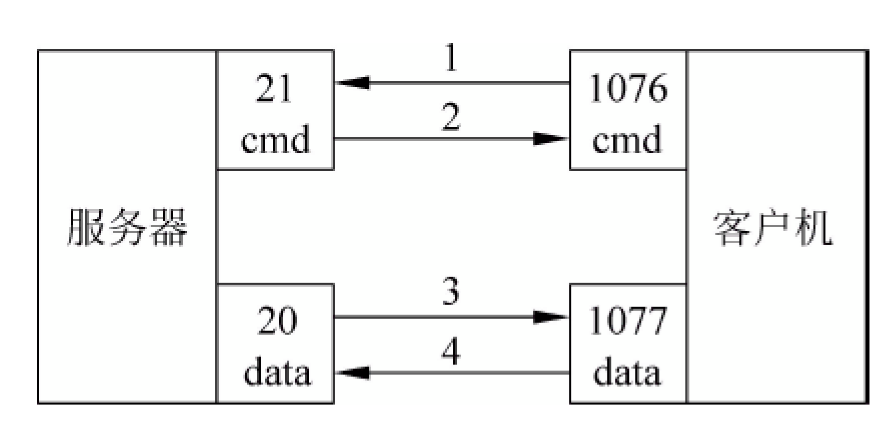


图 8.1 主动 FTP 模式

在图 8.1 的步骤 1 中，客户机打开一个大于 1024 的命令端口 1076 与 FTP 的命令端口 21 建立连接，并通过该连接发送命令“Port 1077”给服务器，使得服务器知道客户机将使用端口 1077 接收 FTP 数据。在步骤 2 中，服务器给客户机的命令端口返回一个“ACK”。在步骤 3 中，当服务器需要传送数据给客户机时，则打开其数据端口 20 连接至客户机的 1077 端口，并使用该连接传输 FTP 数据。步骤 4 中，客户机返回一个“ACK”给服务器。

由于目前很多防火墙不允许外部发起的连接至内部高端端口的请求，所以在很多情况下，当使用 FTP 主动方式时，防火墙内部的客户机无法访问外部的 FTP 服务器，因为 FTP 通过 20 端口发起的与内部主机高端端口的请求被防火墙拒绝了。

2. 被动方式的工作原理

在被动方式的 FTP 中，命令连接和数据连接都由客户端发起。客户机上的 FTP 客户端软件首先开启一个大于 1024 的高端端口与 FTP 服务器的 21 端口建立连接，用于传送控制命令。当客户端需要接收数据时，则向服务器的 21 端口发送 Pasv 命令。当服务器接收到 Pasv 命令后，随机打开一个高端端口(端口号大于 1024)，并且通知客户机连接到此端口来接收数据(服务器的被动连接)。其连接过程如图 8.2 所示。

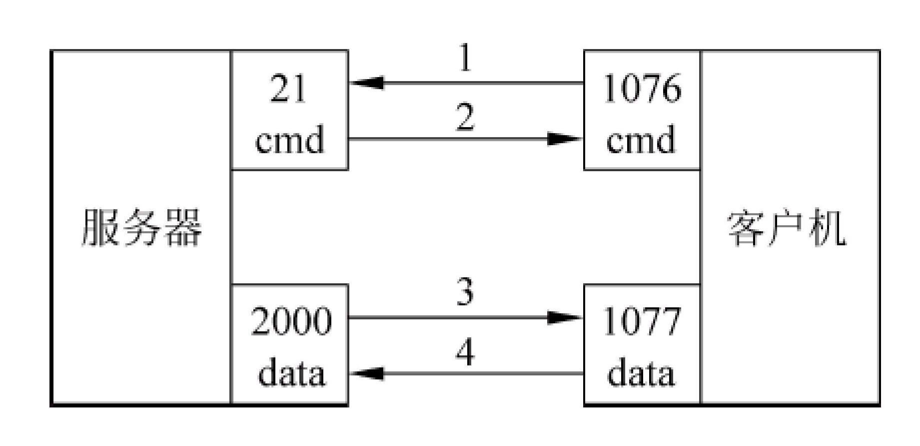


图 8.2 被动 FTP 模式

在图 8.2 的步骤 1 中，客户机打开一个大于 1024 的命令端口 1076 与 FTP 的命令端口 21 建立连接，并通过该连接发送命令“Pasv”给服务器。在步骤 2 中，服务器返回一个“Port 2000”给客户机的命令端口，使得客户机知道服务器将在 2000 端口发送 FTP 数据。步骤 3 中，客户机发起并建立一个从自己的数据端口 1077 到服务器的数据端口 2000 的连接，用于接收来自服务器的 FTP 数据。步骤 4 中服务器返回一个“ACK”给客户机。

在被动 FTP 模式下，解决了放置在客户机前面的防火墙所带来的无法访问的问题。但是这种方式下，客户机能够连接至服务器的高端端口，对服务器的安全性造成了潜在威胁。针对这种问题，目前许多 FTP 守护进程允许管理员制定 FTP 服务器使用的端口范围。

8.4 实验内容

本章的实验内容包括以下 5 部分：

(1) 演示如何在 Windows 2003 系统中安装 FTP 服务。

(2) 演示如何在 Internet 信息服务(IIS)管理器中部署 FTP 服务。

(3) 演示如何设置访问 FTP 站点的用户账号。

(4) 演示如何设置匿名访问 FTP 站点的方法。

(5) 演示当出现授权用户无法访问 FTP 站点时的一般解决方法。

8.5 实验步骤

8.5.1 安装 FTP 服务

在 Windows 2003 服务器中插入系统安装盘。单击"控制面板"→"添加或删除程序"，在弹出的"添加或删除程序"对话框的右边单击"添加/删除 Windows 组件"，出现"Windows 组件向导"对话框后，选中"应用程序服务器"，然后选择"详细信息"，弹出"应用程序服务器"对话框，选择"Internet 信息服务"，单击"详细信息"打开"Internet 信息服务"对话框，在"文件传输协议(FTP)服务"前打钩，如图 8.3 所示。单击"确定"按钮，然后根据提示信息安装 FTP 服务。

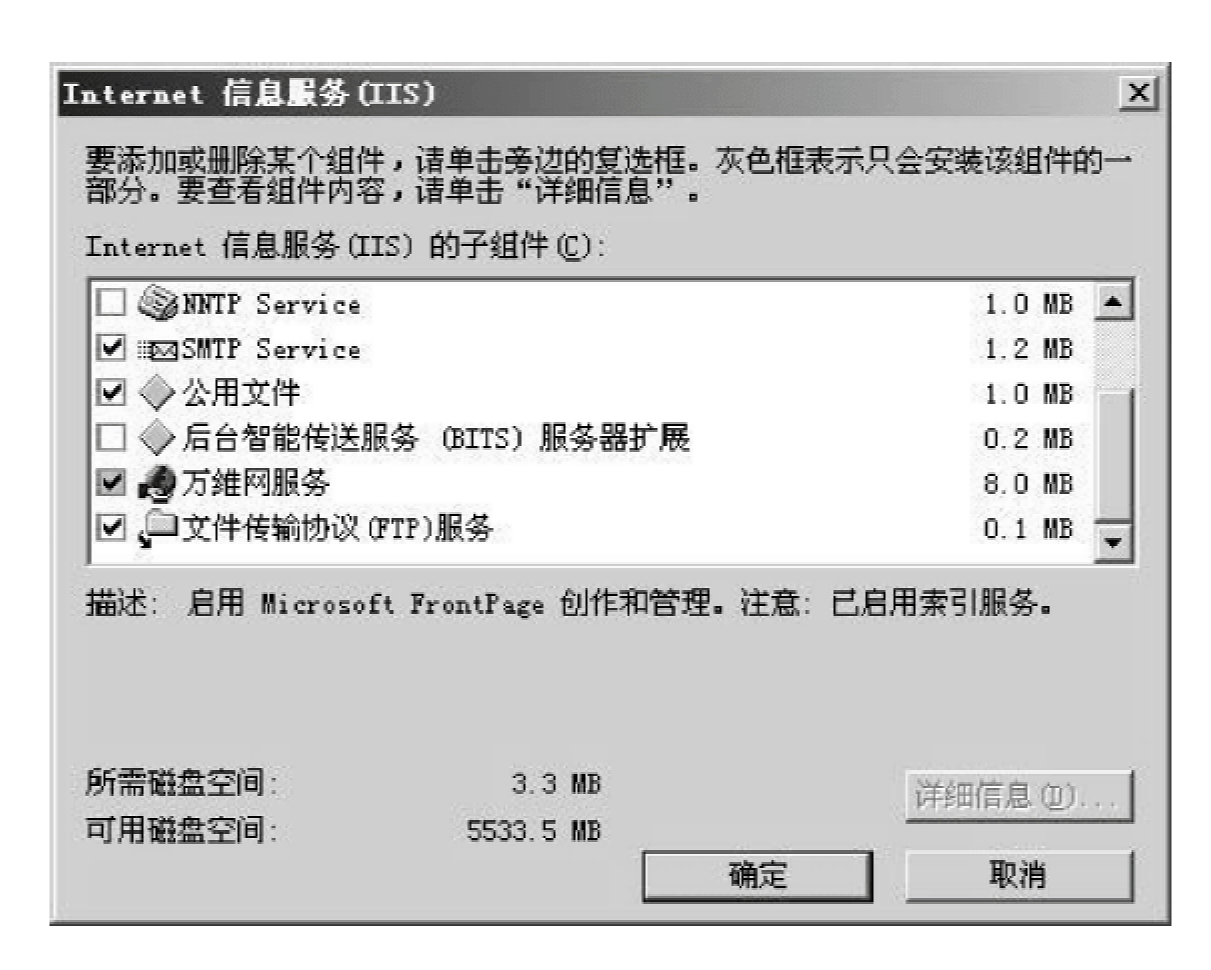


图 8.3 安装 FTP 服务

8.5.2 设置 FTP 站点

打开"Internet 信息服务(IIS)管理器"，如图 8.4 所示。

在"Internet 信息服务(IIS)管理器"中右键单击"FTP 站点"，在弹出的快捷菜单中选择"属性"，打开"默认站点 属性"对话框。在"FTP 站点"属性页中可以设置 FTP 站点的名称。

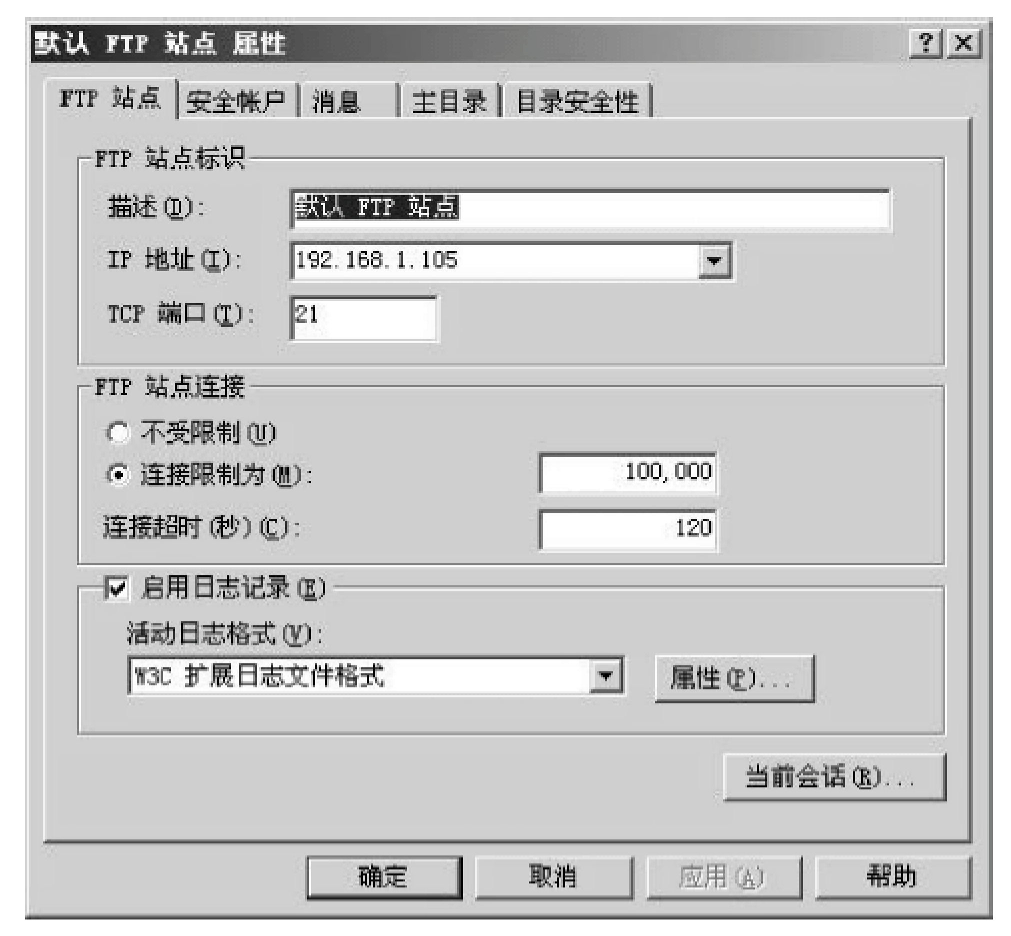




图 8.4　打开 IIS 管理器

将“IP 地址”设置为服务器的 IP，“TCP 端口”设置为“21”，如图 8.5 所示。

选择“主目录”属性页，设置存放 FTP 文件的目录、访问目录的方式以及在客户端中打开该目录时的显示方式，如图 8.6 所示。



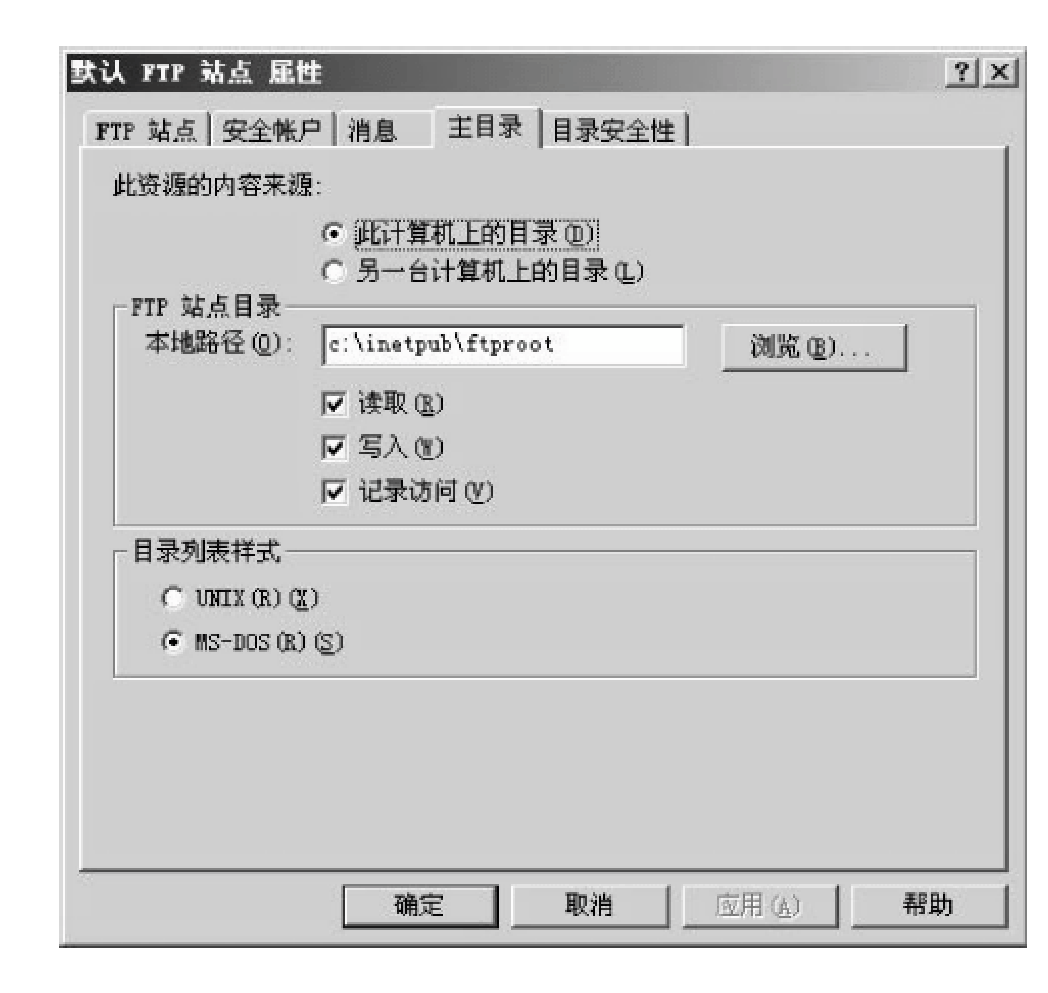


图 8.5　设置 FTP 站点的 IP 地址、端口号

图 8.6　“主目录”的设置

注：“默认站点 属性”中的写入权限高于用户的写入权限，若在这里不选上“写入”，任何用户将无法写入 FTP 站点。

8.5.3　设置 FTP 账户

在任务栏中单击“开始”→“运行”命令，输入 cmd 命令，打开控制台。在控制台中使用 net user 命令创建三个账户 user1、user2 和 user3，如图 8.7 所示(在后续的步骤中，将 user1 设置为仅有“读取”权限的匿名账户；user2 设置为具有“读取”和“写入”权限的账户；user3 设置为具有“完全控制”权限的账户)。

在“Internet 信息服务(IIS)管理器”中选择“FTP 站点”→“默认站点”，右键单击“默认站点”，在弹出的快捷菜单中选中“权限”，如图 8.8 所示。



图 8.7 添加账户



图 8.8 选择“权限”命令

在弹出如图 8.9 所示的对话框中，单击“添加”按钮。

在弹出的“选择用户和组”对话框中依次单击“高级”→“立即查找”按钮，然后按住 Ctrl 键，在列出的搜索结果中将 user1、user2 和 user3 全部选中，单击“确定”按钮，如图 8.10 所示。

依次选中 user1、user2 和 user3，并分别设置它们的权限。其中 user1 的允许权限为“读取”；user2 的允许权限为“读取”和“写入”；user3 的允许权限为“完全控制”。图 8.11 给出了 user1 的权限设置方式。



图 8.9 “权限设置”对话框



图 8.10 选择用户 user1、user2 和 user3



图 8.11　设置 user1 的权限

打开 Windows XP 的 IE 浏览器，在地址栏中输入“FTP：//192.168.1.105”，在弹出的“登录身份”对话框中输入用户名为 user1 及密码为 123，单击“登录”按钮，则以 user1 的身份登录 FTP 服务器，如图 8.12 所示。

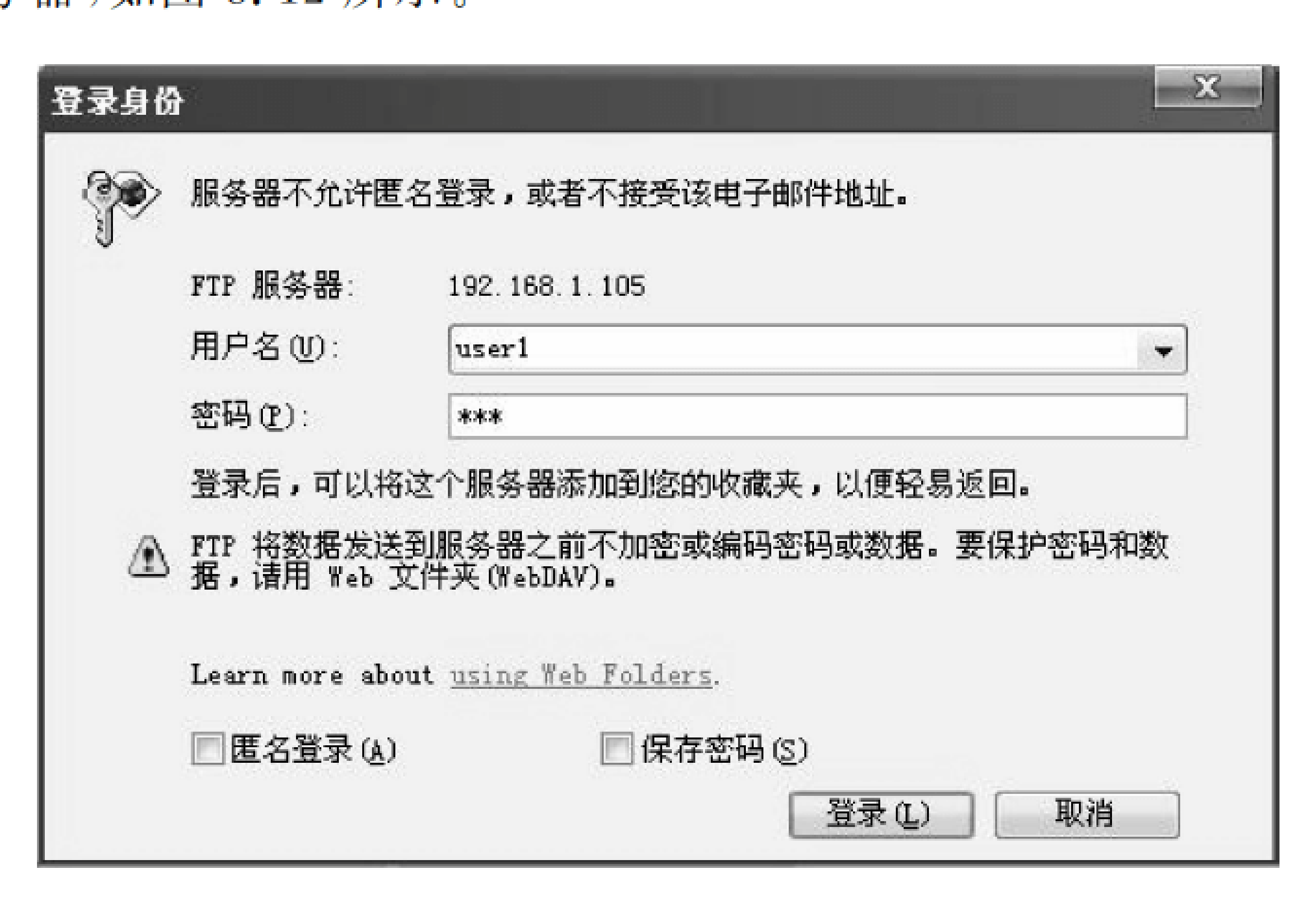


图 8.12　登录 FTP 服务器

以 user1 的身份在服务器目录中修改文件夹“文件夹 1”的名称时，出现的错误提示如图 8.13所示。由于 user1 仅有“读取”服务器目录的权限，因此只能查看服务器目录中的内容。



图 8.13 越权访问的错误提示

8.5.4 设置匿名账户

在“默认站点 属性”对话框中选择“安全账户”属性页，选中“允许匿名连接”。单击“浏览”按钮，在弹出的对话框中选择 user1 账户(具体操作参见图 8.7 和图 8.8)，将其作为匿名账户，并输入 user1 的登录密码，如图 8.14 所示。此后，当在客户端打开 IE，在地址栏中输入 FTP：//192.168.1.105 时，则自动以 user1 登录，并仅具有“读取”权限。



图 8.14 匿名账户的设置

8.5.5 FTP 账户的访问权限

当 FTP 的管理员将一个目录复制到 FTP 的站点目录上供用户下载时，往往会出现用户无法访问该文件的情况。这种情况的发生一般是由于 FTP 的站点目录放置在 FTP 服务器的 NTFS 分区上，而在该分区上没有设置用户的账户访问该目录的权限。

比如，在 FTP 服务器中，我们将一个目录 SSH_Win 复制到 FTP 的站点目录下，当客户机以匿名方式访问 FTP 服务器时，无法访问到 SSH_Win 目录下的内容，如图 8.15、图 8.16 所示。



图 8.15　访问 FTP 服务器

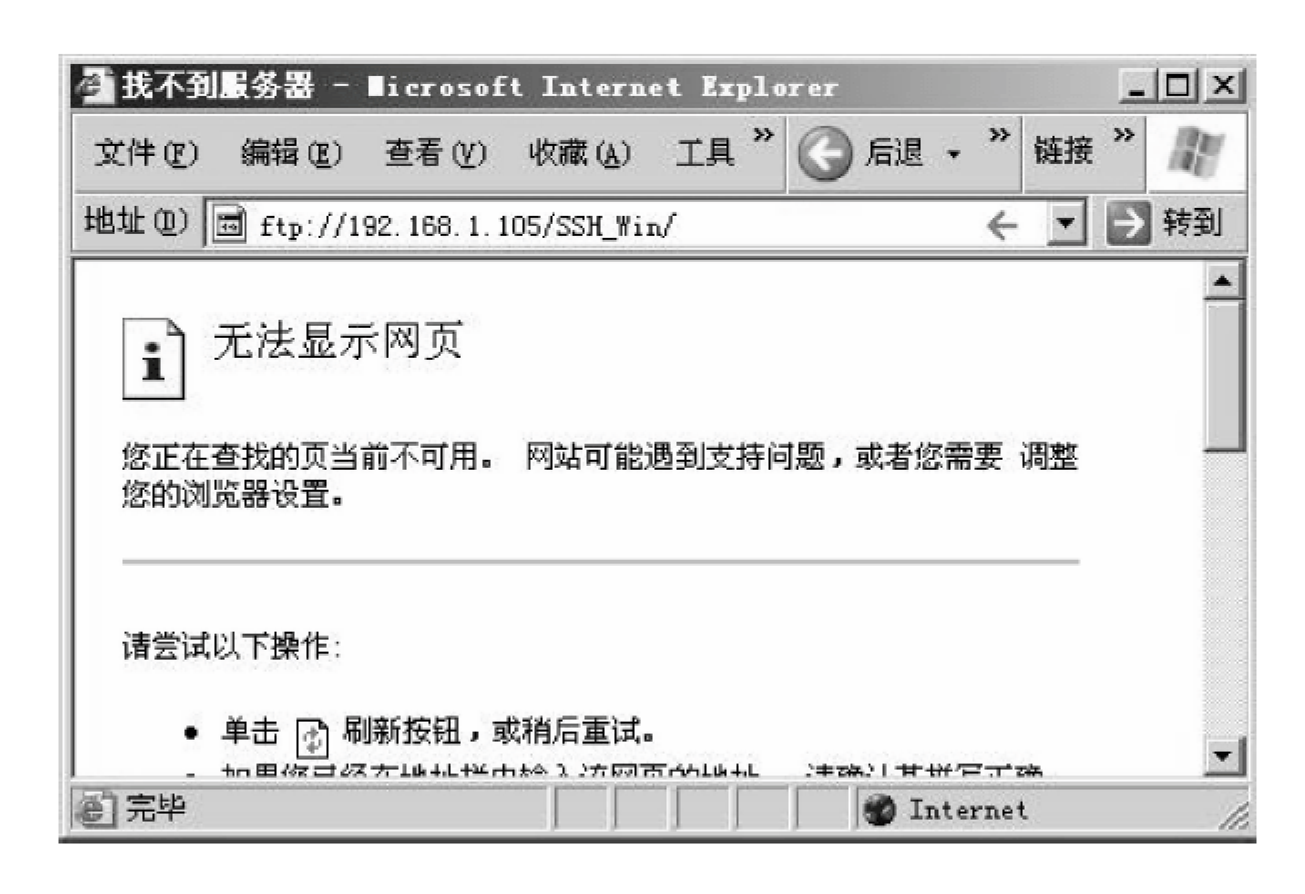


图 8.16　无法打开 FTP 服务器中的 SSH_Win 目录

在 FTP 服务器上的 FTP 站点目录下，右键单击 SSH_Win 目录，在弹出的快捷菜单中选择“属性”，在弹出的 SSH_Win 对话框中选择“安全”选项卡，可以看到在允许访问的“组或用户名称”列表中没有账户 user1(匿名账户)，如图 8.17 所示，这就是用户无法使用匿名账户 user1 访问 SSH_Win 目录的原因。

在“SSH_Win”属性对话框中单击“添加”按钮，在弹出的“选择用户或组”对话框中单击

“高级”按钮，然后单击“立即查找”按钮，如图 8.18、8.19 所示。在出现的“搜索结果”中选择“user1”，然后单击“确定”按钮，如图 8.20 所示，将该账户加入到目录“SSH_Win”的访问列表中，并将其访问权限设置为“读取和运行”、“列出文件夹目录”和“读取”，如图 8.21 所示。



图 8.17　SSH_Win 的访问列表



图 8.18　“选择用户或组”对话框



图 8.19　查找用户或组



图 8.20 选择账户 user1

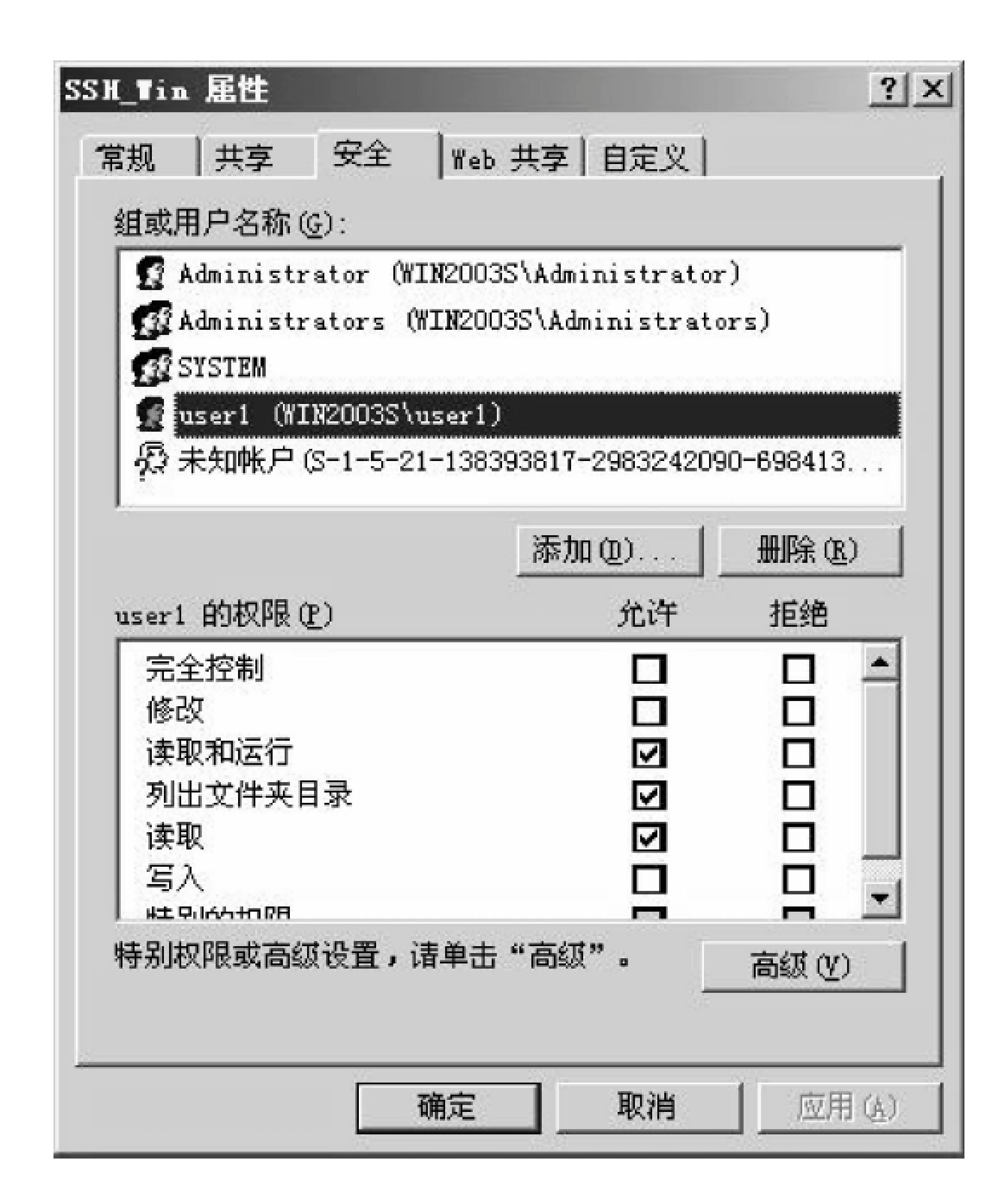


图 8.21 设置 user1 的访问权限

此时，在客户中通过匿名账户就可以访问 SSH_Win 目录了，如图 8.22 所示。



图 8.22 匿名访问 SSH_Win 目录

8.6 实验思考

（1）挂接虚拟目录时，如何设置默认挂接到各授权用户的主目录？

（2）在服务器端如何设置成允许用户修改密码？用户在客户端如何修改密码？

实验9 网络嗅探实验

9.1 实验目的与要求

- 理解网络嗅探的原理。
- 掌握 Windows 操作系统下 Sniffer Pro 工具的使用方法。
- 掌握如何使用 Sniffer Pro 工具分析网络协议。

9.2 实验环境

在 VMWare 虚拟机中安装操作系统 Windows 2003、Windows XP 以及 Windows 2000，其中 Windows 2003 配置成 FTP 服务器，Windows XP 作为 FTP 客户机，Windows 2000 安装网络嗅探工具 Sinffer Pro。将 3 种操作系统配置到一个局域网中。

9.3 预备知识

9.3.1 网络嗅探

网络适配器是用于在网络上收发数据的硬件设备，每块网络适配器均具有全球唯一的硬件地址(MAC 地址)。当发送数据时，网络适配器将数据通过广播的方式向外传递；当接收数据时，网络适配器根据接收数据的目的 MAC 地址以及网络适配器驱动程序设置的接收模式进行判断，当数据适合接收时，则产生中断信号发送给 CUP，然后由操作系统调用驱动程序进行接收；当数据不适合接收时，网络适配器则直接丢弃该数据。

网络适配器一般有 4 种工作模式：

- 广播模式(Broadcast)　能够接收网络中的广播数据。
- 多播方式(Multicast)　当数据包的目的地址为多播地址，而且网络适配器地址是属于那个多播地址所代表的多播组时，网络适配器将接纳此数据包，即使一个网络适配器并不是一个多播组的成员，程序也可以将其设置为多播模式而接收那些多播的数据包。

- 直接模式(Directory) 当有数据包的目的 MAC 地址为网络适配器自己的地址时，才能接收它。
- 混杂模式(Promiscuous) 网络适配器将接收所有经过它的数据包。
- 网络适配器的默认工作模式包含广播模式和直接模式，即它只接收广播数据包和发给自己的数据包。而当将网络适配器的工作模式设置为混杂模式时，则可以进行网络嗅探(Sniffer)。

所谓网络嗅探就是将网络适配器设置为混杂模式，截获每一个经过本网络适配器的数据包，然后对数据包进行解码，获取数据包中包含的应用层数据。网络嗅探工具是网络管理员使用的一种有力工具，借助于该工具，能够分析网络协议中的各种数据，了解网络中流量的变化，掌握网络的运行情况，及时发现网络中存在的问题。同时，网络嗅探工具也能捕获网络中以明文形式传输的敏感信息，如用户名、密码、银行卡账号及其他信息，造成网络信息安全问题。但是在使用了路由设备的网络中，由于数据包是根据目的地址进行转发，单个网络适配器将无法监听到所有正在传输的信息。因此 Sniffer 工具所能监听到的数据包仅限于在同一物理网络内传送的数据。

网络嗅探工具分为两种，软件形式的工具有 Sniffer Pro、WireShark、NetXray、PackerBoy 等，易于学习使用，但无法获取所有网络上传输的数据，某些情况下也就可能无法真正了解网络的故障和运行情况，价格便宜；硬件形式的工具通常称为协议分析仪，能够准确了解网络的运行情况和存在故障，价格高。

9.3.2 ICMP 协议

ICMP 协议全称为 Internet Control Message Protocl，是 TCP/IP 协议簇中隶属于网络层的一个子协议。该协议主要用于在主机和路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标、IP 路由器无法按照当前的传输速率转发数据包等情况时，会自动发出 ICMP 消息，这弥补了 IP 协议作为一个无连接协议不能处理网络故障的缺陷。一般而言，ICMP 报文主要针对网络层提供错误诊断、拥塞控制、路径控制和检测服务 4 大功能。

- 错误诊断 当网络中的主机或者整个网络由于故障不可达时，会产生 ICMP 报文通告这一事实。
- 拥塞控制 当路由器发送数据包的速度慢于接收数据包的速度时，路由器中会缓存大量的数据包，此时会产生“ICMP 源结束”消息，该消息可以降低发送方发送数据包的速度，以缓解网络拥塞。但由于“ICMP 源结束”消息的持续发送也会造成网络拥塞，因此该功能的使用较为慎重。
- 路径控制 当一个 IP 包在网络中传输时，每经过一个路由器，其 TTL(Time to Live，生存期)值就会减一，当 TTL 值降为零时，路由器就会丢弃该 IP 包，此时会产生一个 ICMP 报文来通告这一事实。TraceRoute 工具是一个 Windows 操作系统内置的跟踪路由的小工具，它就是通过发送 IP 包并监视 ICMP 超时通告来显示路由信息的。
- 检测服务 ICMP 消息中有两类子消息：回显消息(echo request)与回显响应消息

(echo reply),利用这两类消息可以检测网络是否通畅。Ping 命令就是利用了这两类子消息来检测目标主机是否可达的。

ICMP 协议的报头结构如图 9.1 所示。

其中:

- 类型 标识生成的错误报文,它是 ICMP 报文中的第一个字段。
- 代码 进一步限定生成 ICMP 报文。该字段可用于查找产生错误的原因。
- 校验和 存储了 ICMP 所使用的校验和值。
- 未使用 保留字段,供将来使用,起值设为 0。
- 数据 包含所有接收到的数据报的 IP 报头,此外还包含 IP 数据报中前 8 个字节的数据。



图 9.1 ICMP 报头结构

ICMP 协议提供的诊断报文类型如表 9.1 所示。

表 9.1 ICMP 诊断报文类型

类 型	描 述
0	回应应答(Ping 应答,与类型 8 的 Ping 请求一起使用)
3	目的不可达
4	源消亡
5	重定向
8	回应请求(Ping 请求,与类型 0 的 Ping 应答一起使用)
9	路由器公告(与类型 10 一起使用)
10	路由器请求(与类型 9 一起使用)
11	超时
12	参数问题
13	时标请求(与类型 14 一起使用)
14	时标应答(与类型 13 一起使用)
15	信息请求(与类型 16 一起使用)
16	信息应答(与类型 15 一起使用)
17	地址掩码请求(与类型 18 一起使用)
18	地址掩码应答(与类型 17 一起使用)

ICMP 提供多种类型的消息,为源端节点提供网络层的故障信息反馈,它的报文类型可以归纳为以下 5 个大类:

- 诊断报文(类型 8,代码 0;类型 0,代码 0)。
- 目的不可达报文(类型 3,代码 0～15)。
- 重定向报文(类型 5,代码 0～4)。
- 超时报文(类型 11,代码 0～1)。
- 信息报文(类型 12～18)。

9.4 实验内容

本章的实验内容主要包括以下 3 部分：

(1) 演示如何通过设置 Sniffer 工具和开启 Ping 命令来捕获 ICMP 数据包。

(2) 演示如何根据捕获的数据包对 ICMP 协议进行分析。

(3) 演示如何对一次 FTP 的登录过程进行数据包的抓取和分析，同时演示如何分析出账户的登录密码。

9.5 实验步骤

9.5.1 ICMP 协议数据的捕获

1. 设置协议过滤器

打开 Sniffer Pro 工具，在菜单栏中单击 Capture 菜单项，在弹出的下拉菜单中选中 Define Filter 命令，如图 9.2 所示。

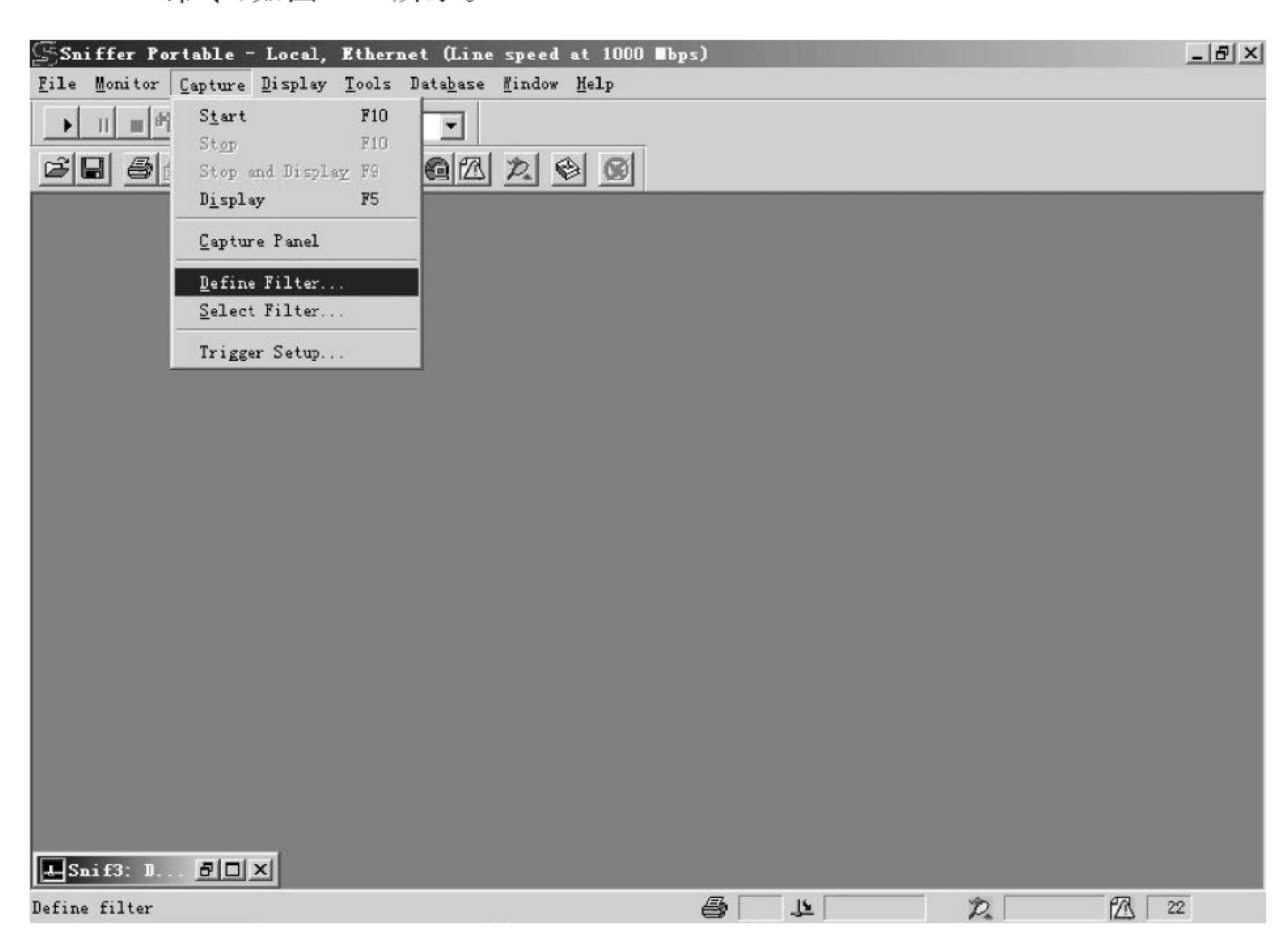


图 9.2 定义过滤器

在弹出的 Define Filter-Capture 对话框中选择 Advanced 属性页，在窗口中选择“IP 协议”，然后单击“IP”协议前的加号，在展开的协议中选择“ICMP 协议”，如图 9.3 所示。

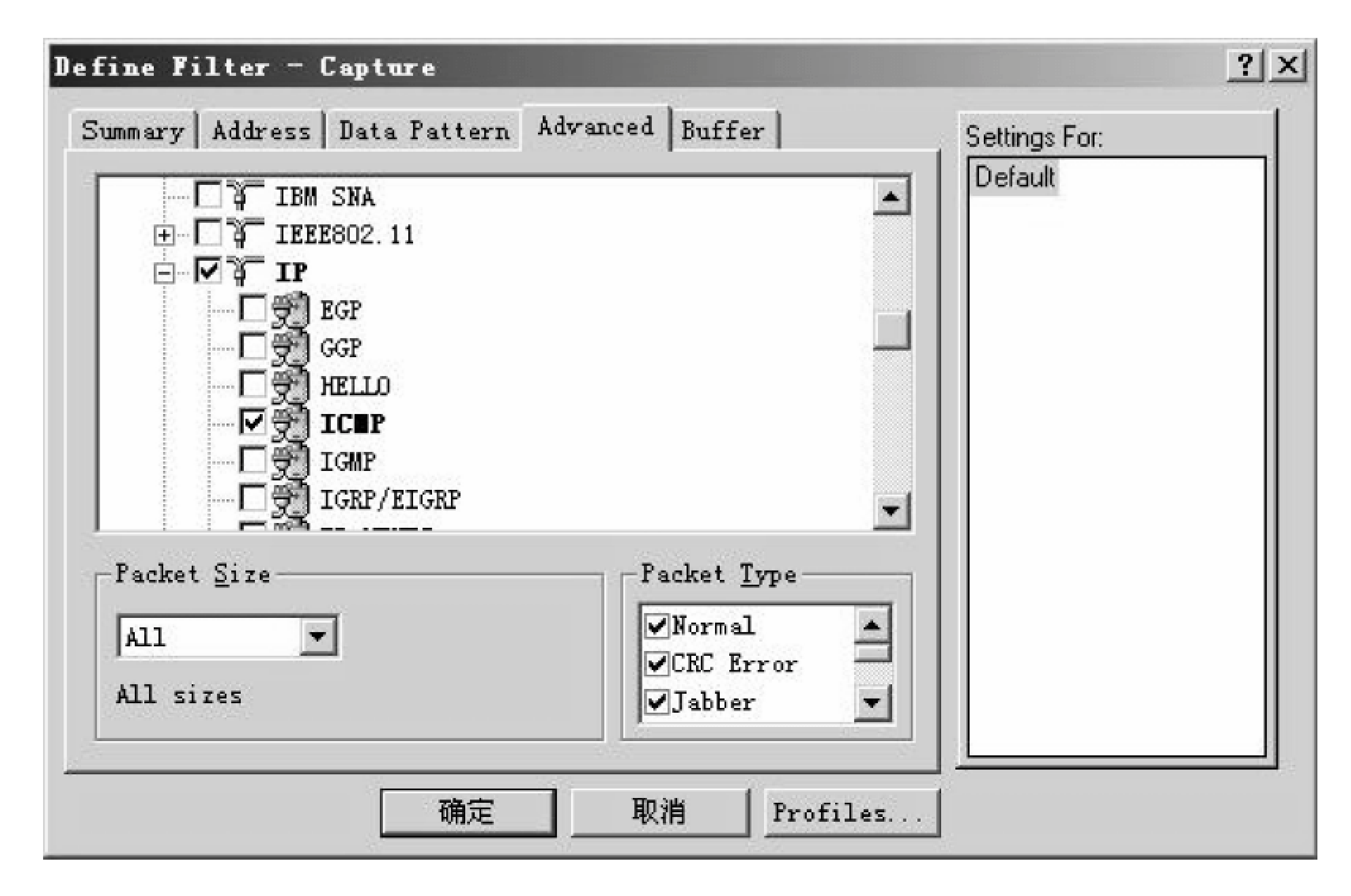


图 9.3 设置协议过滤器

2. 打开 Traffic Map 视图

在 Sniffer Pro 的主窗口中选择 Monitor 下拉菜单，然后选择该菜单中的 Matrix 命令，就会看到关于网络的 Traffic Map 视图，如图 9.4 所示。

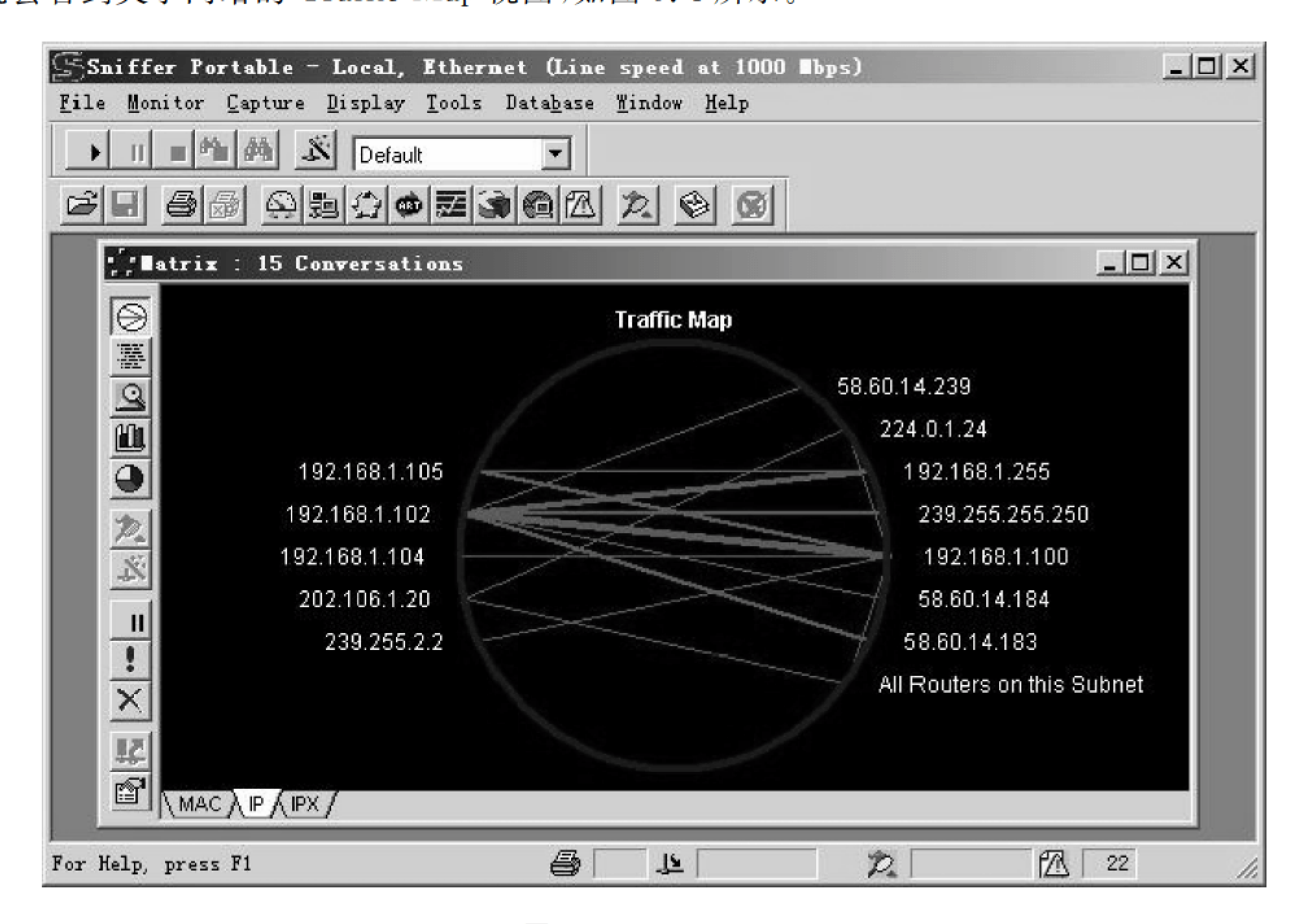


图 9.4 Traffic Map

3. 设置监听目标

在 Traffic Map 视图中用鼠标选中要捕获数据的 IP 地址 192.168.1.102，将其反白显示，然后在该 IP 地址处单击鼠标右键，在弹出的快捷菜单中选择 capture 命令，如图 9.5 所示。此时，Sniffer Pro 进入数据监听阶段。

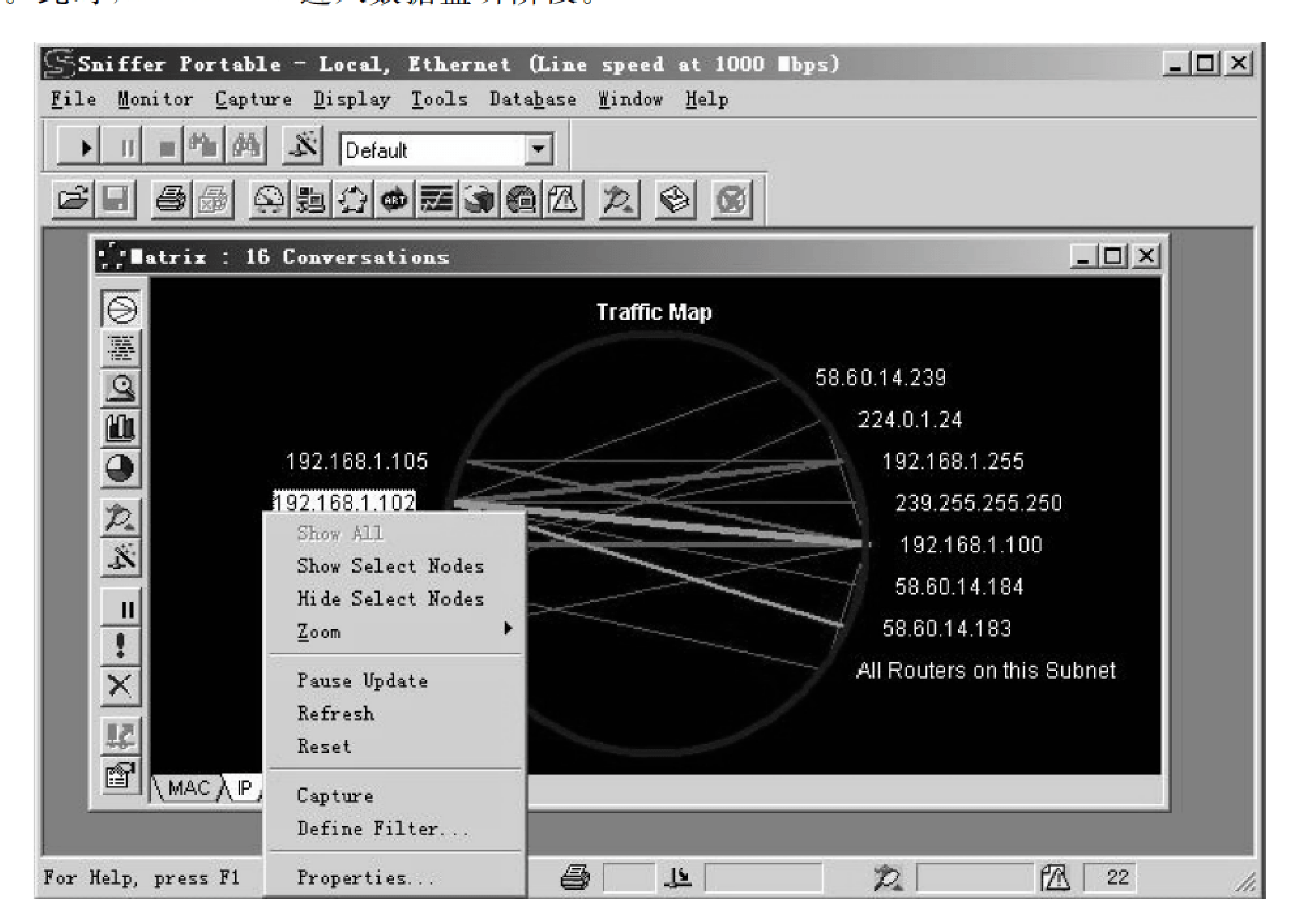


图 9.5 设置需要监听的目标主机

4. 运行 Ping 命令

在 IP 地址为 192.168.1.102 的主机上，依次单击"开始"→"运行"命令，在弹出的"运行"对话框中输入 cmd 命令并单击"确定"按钮，然后在弹出的控制台窗口中输入 Ping 192.168.1.104，按 Enter 键，如图 9.6 所示。

5. 协议分析

返回 Sniffer Pro 所在的主机，在 Sniffer Pro 的主界面上单击 stop and dispaly 按钮，停止抓包，并在弹出的窗口中选择左下角的 decode 选项，窗口中会显示所捕获到的数据，如图 9.7所示。

9.5.2 ICMP 协议的分析

在图 9.7 中会看到 3 个窗口，最上面的窗口显示了所捕获数据包的源 IP 地址、目的 IP 地址以及数据包的描述。当选中其中一条数据后，会在中间窗口和底部窗口中分别显示分

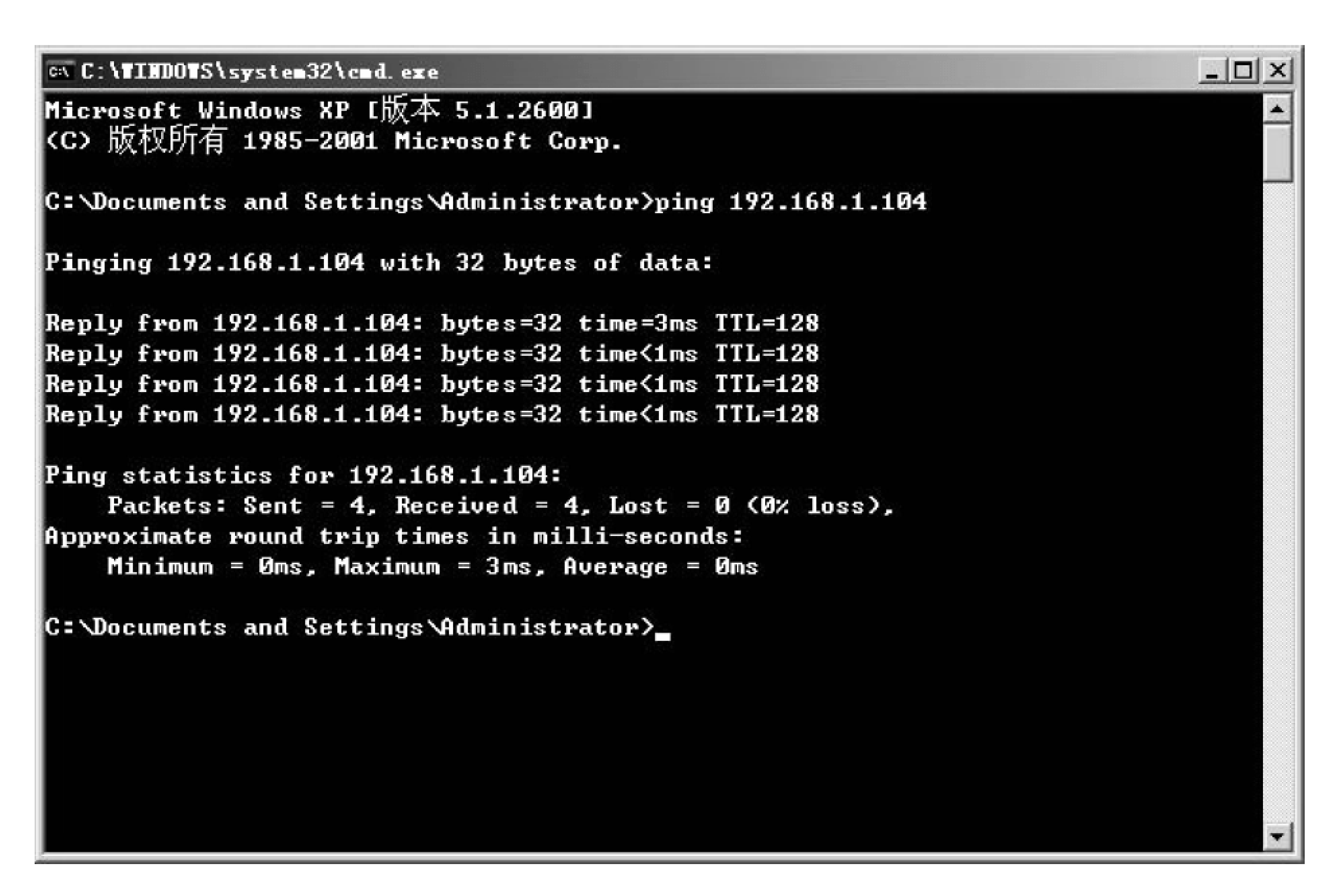


图 9.6　执行 Ping 命令

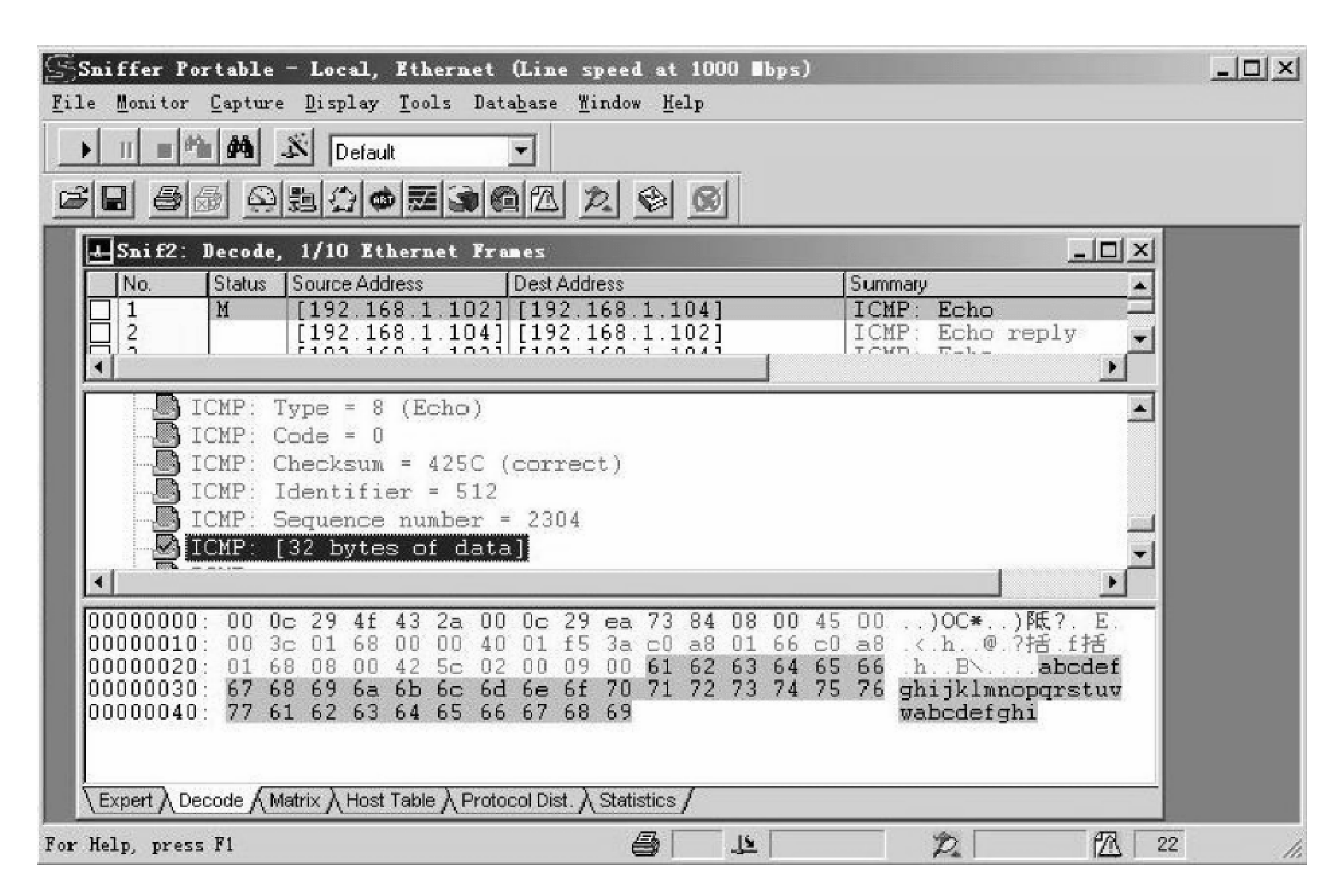


图 9.7　Decode 窗口

析数据和原始数据。

(1) 在最上面的窗口中选中第一条数据,从其描述(Summary 列)可以看出它是一条回显消息,是从 IP 地址 192.168.1.102 发往 192.168.1.104。从中间的窗口中可以看出该数据的类型是 8,代码是 0,其序列号为 2304。当选中数据区时,在底部窗口中会显示具体的原始数据。

(2) 在最上面的窗口中选中第二条数据,从其描述列可以看出它是一条回显应答消息,是从 IP 地址 192.168.1.104 发往 192.168.1.102。从中间的窗口可以看出该数据的类型为 0,代码为 0,序列号为 2304,这说明该回显应答消息与第一条的回显消息是对应的,如图 9.8 所示。

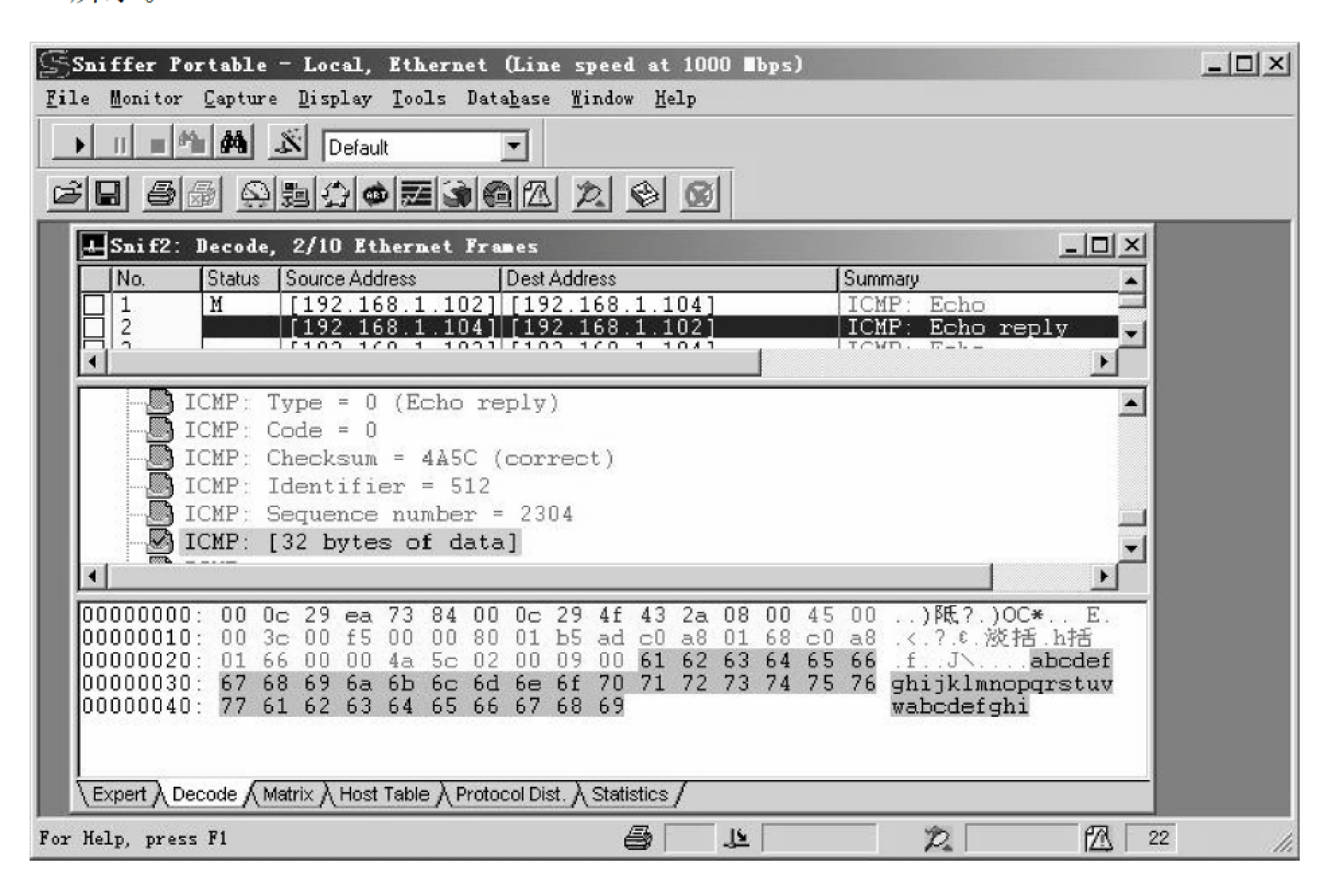


图 9.8 回显应答消息

9.5.3 FTP 协议数据的捕获和分析

由于要捕获 FTP 数据,因此需要重新设置协议过滤器。在 Define Filter-Capture 对话框的 Advanced 属性页中首先选择“IP”协议,然后单击“IP”协议前的加号,在展开的协议中依次选择“TCP”协议与“FTP”协议,如图 9.9 所示。

通过 Monitor 菜单下的 Matrix 命令打开 Traffic Map 视图,在该视图中选择 192.168.1.102 作为被监听的主机(192.168.1.102 为 FTP 的客户机),然后在该 IP 上单击右键,在弹出的快捷菜单中选择“Capture”命令,进入数据包的捕获状态。

在 FTP 客户机中打开 IE 浏览器,在地址栏中输入 FTP://192.168.1.105,然后敲击 Enter 键,在弹出的“登录身份”对话框中输入用户名与密码。最后单击“登录”按钮,如图 9.10 所示。

在 FTP 客户机登录成功后,切换到安装 Sniffer Pro 的主机,并在 Sinffer Pro 的工具栏

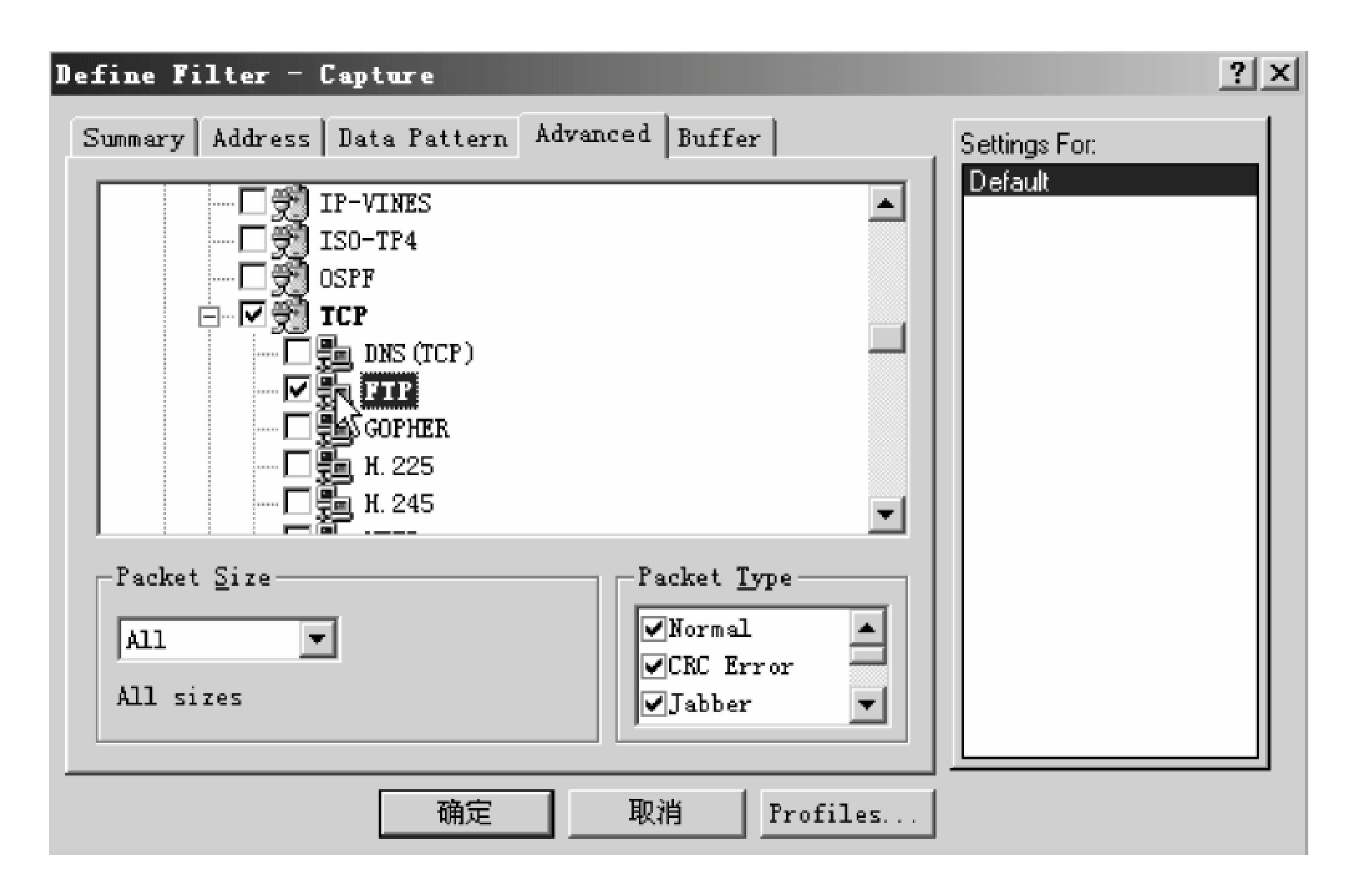


图 9.9 选择 FTP 协议

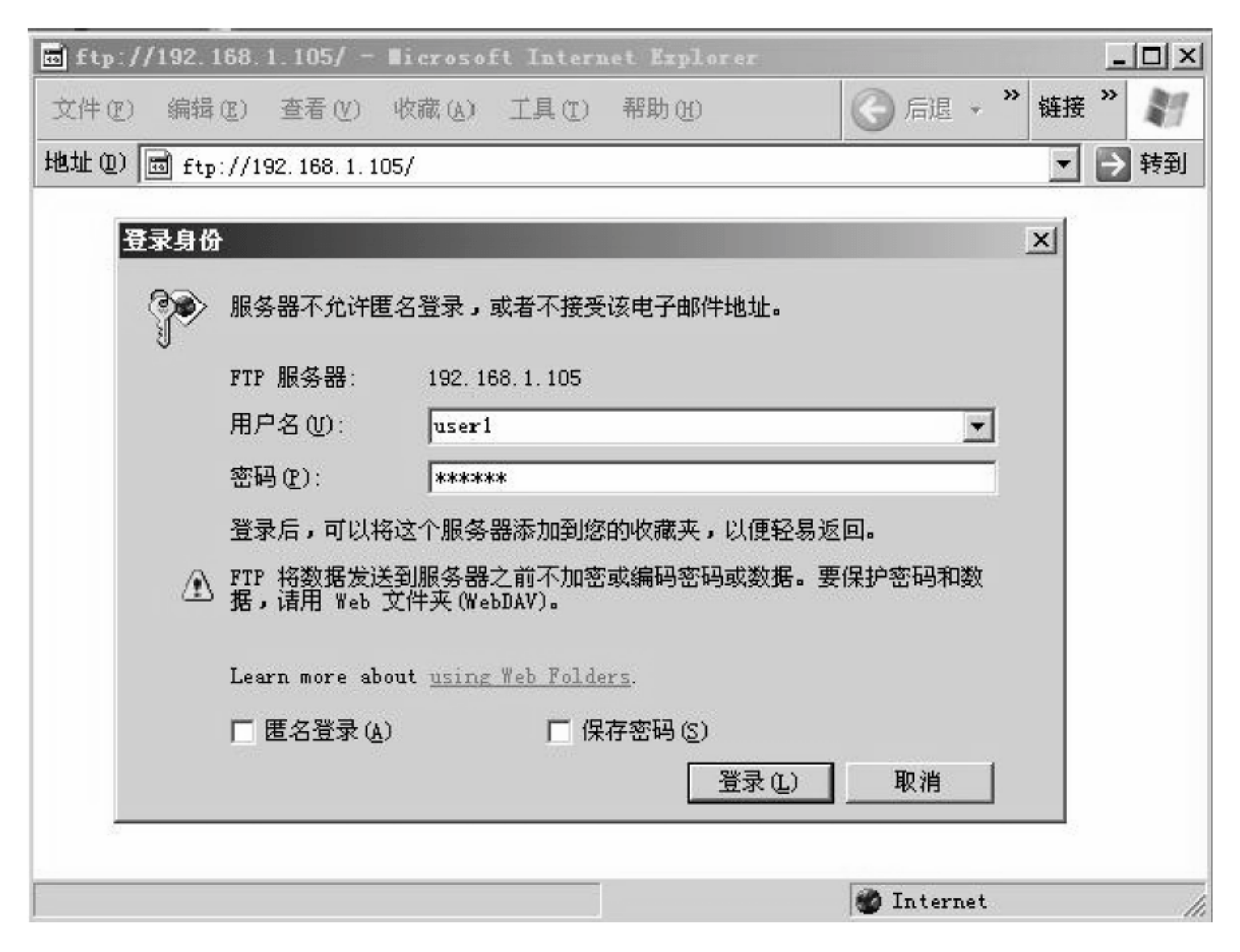


图 9.10 在客户机上登录 FTP 服务器

中单击 Stop and Display 按钮，打开协议分析窗口，选择窗口下方的 Decode 选项卡，进入 FTP 协议的分析界面，如图 9.11 所示。

从图 9.11 可以看出，在捕获的数据包中数据包 1、2、3 显示了一个 TCP 连接过程中的三次握手过程。在最上面的窗口中选中第一条数据(源地址为 192.168.1.102，目的地址为 192.168.1.105)，在中间的窗口中可以看到，第一条数据的源端口为 1102(Source port=

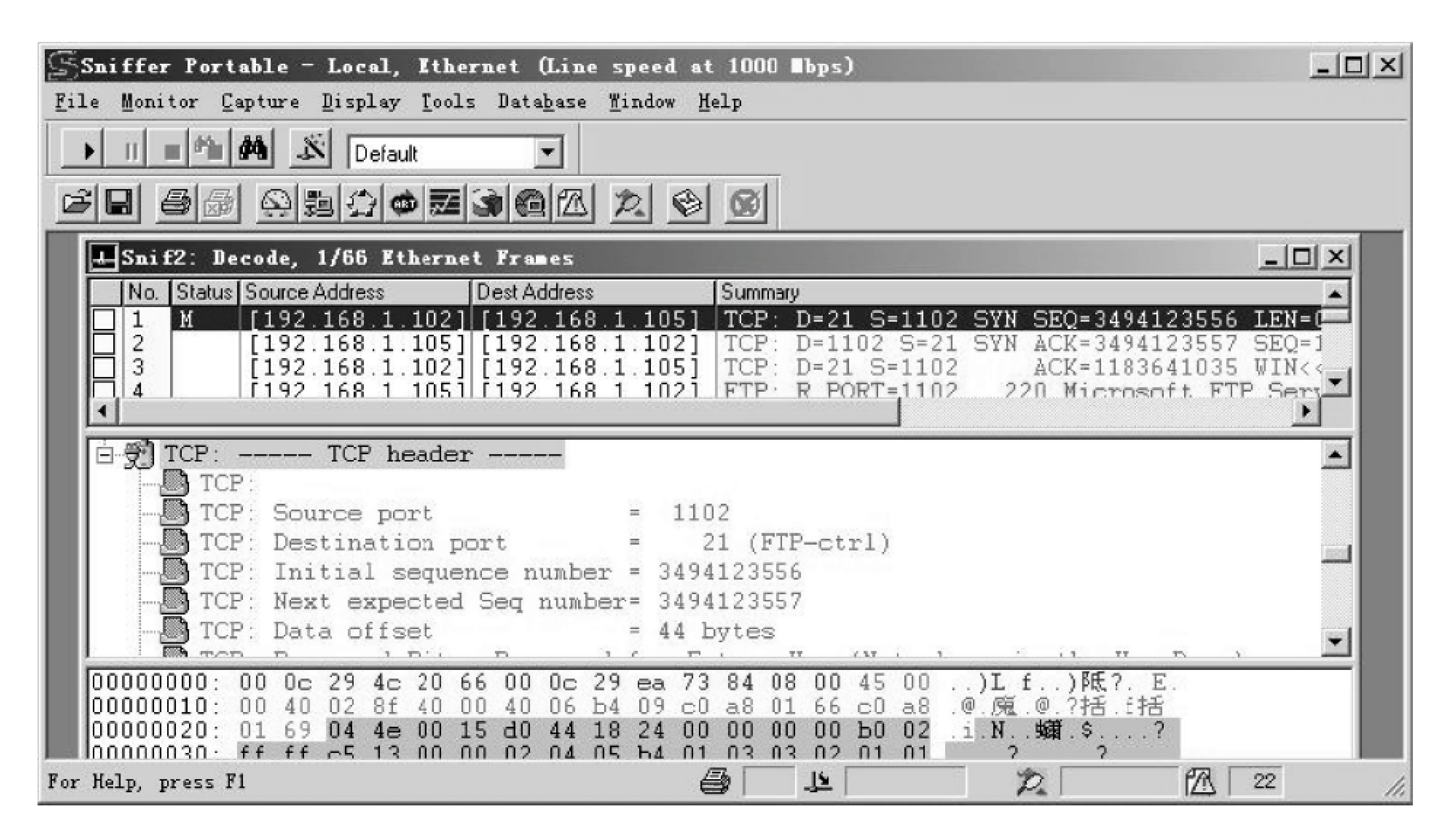


图 9.11 FTP 协议的 Decode 窗口

1102)，目的端口为 21(Destination port = 21)，数据包的序列号为 3494123556(Initial sequence number = 3494123556)，期待收到的数据包的序列号为 3494123557(Next expected Seq number=3494123557)。在最上面的窗口选中第二条数据(如图 9.12 所示)，在中间的窗口中可以看到第二条数据的源端口为 21，目的端口为 1102，其初始序列号为 1183641034，期望接收到的数据的序列号为 1183641035，其确认序列号为 3494123557，与目的地址(192.168.1.102)所期待接收的数据包的序列号一致。从第三条数据也可以看出(如图 9.13 所示)，其确认序列号为 1183641035，与目的地址(192.168.1.105)期待接收的数据包的序列号一致。至此，TCP 的三次握手结束。

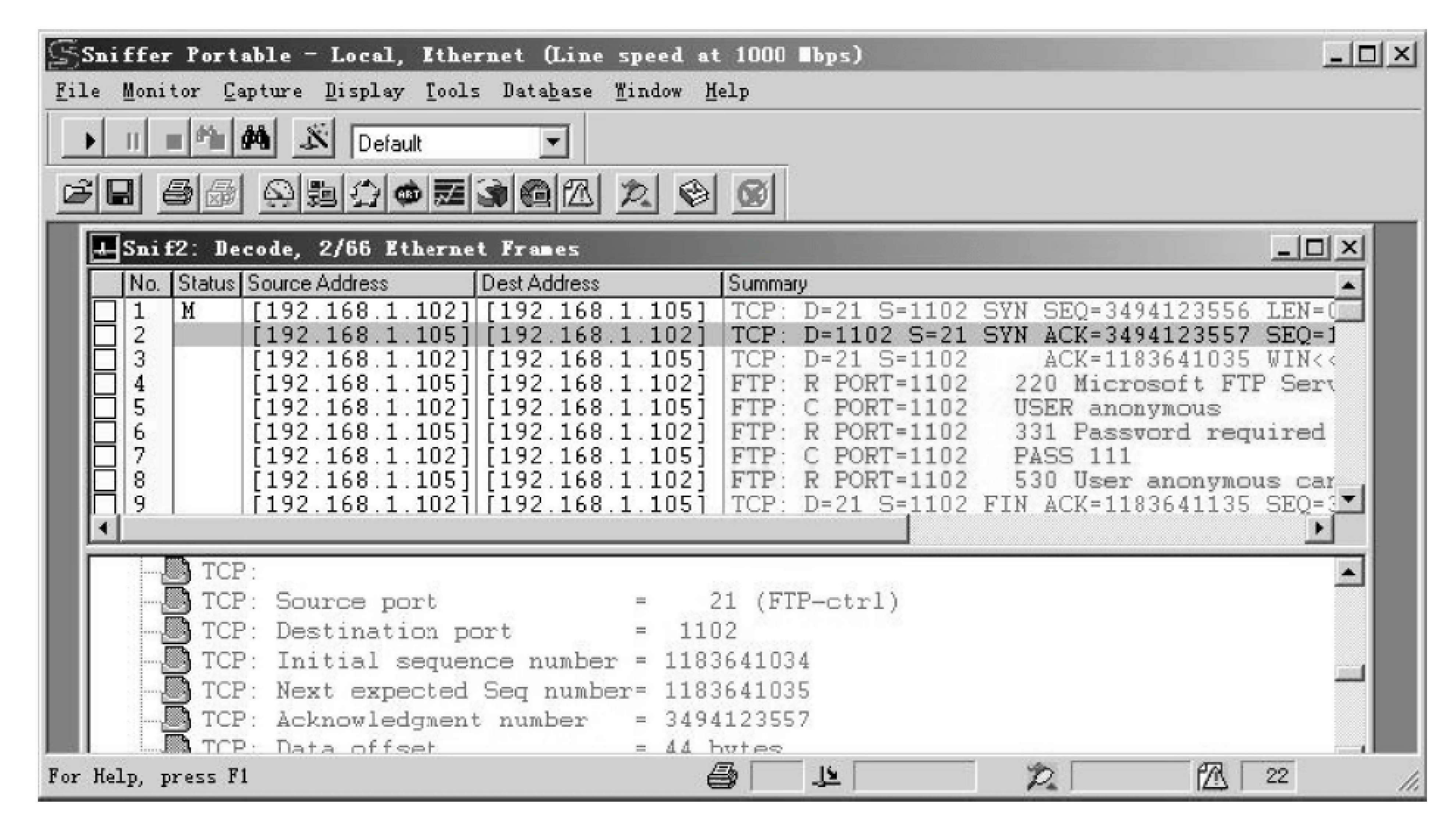


图 9.12 TCP 三次握手的第 2 条消息

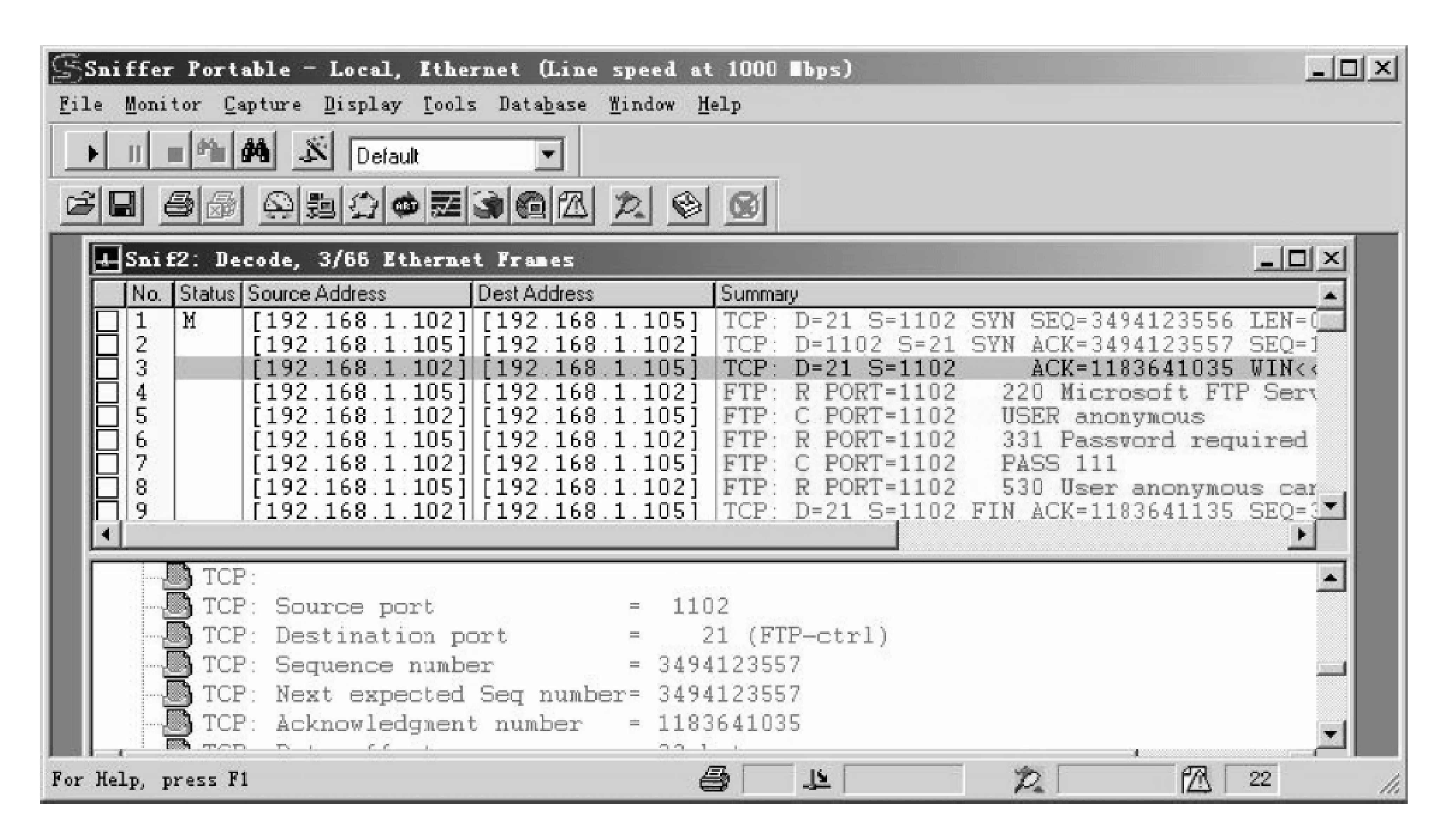


图 9.13 TCP 握手的第 3 条消息

如图 9.14 所示，从 FIN 标识可以看出第 9 条到第 12 条数据显示了一个 TCP 连接结束的 4 个基本步骤。数据包 9 显示出 FTP 客户机(192.168.1.102)向 FTP 服务器(192.168.1.105)发出请求结束此次 TCP 连接。数据包 10 是 FTP 服务器对客户机的确认数据包。数据包 11 是 FTP 服务器向客户机发出的断开 TCP 连接的请求数据包，数据包 12 为客户机向服务器发出的结束连接的确认包。从图 9.15、图 9.16 和图 9.17 可以看出这些数据包的序列号是相互对应的。

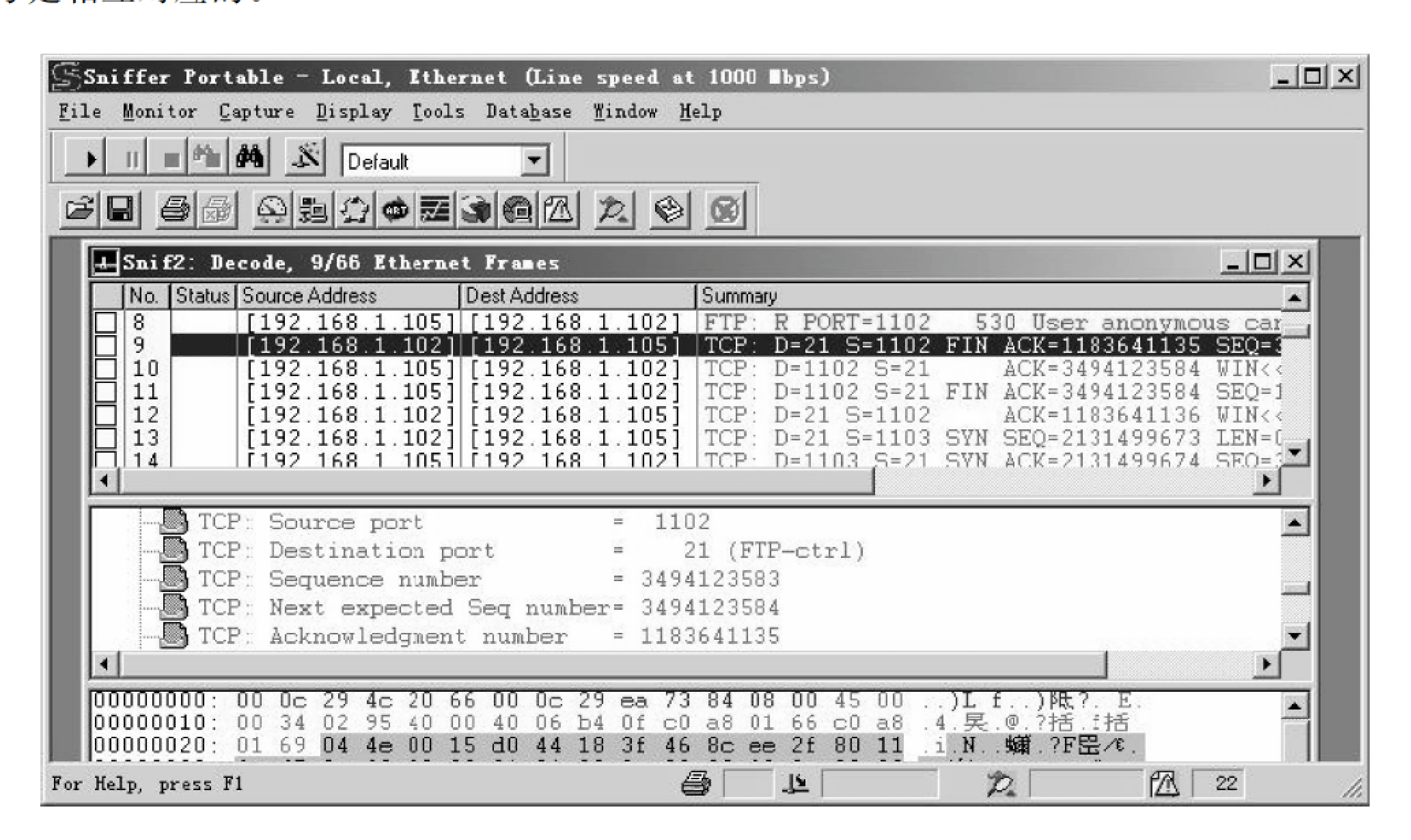


图 9.14 第 1 条 FIN 消息

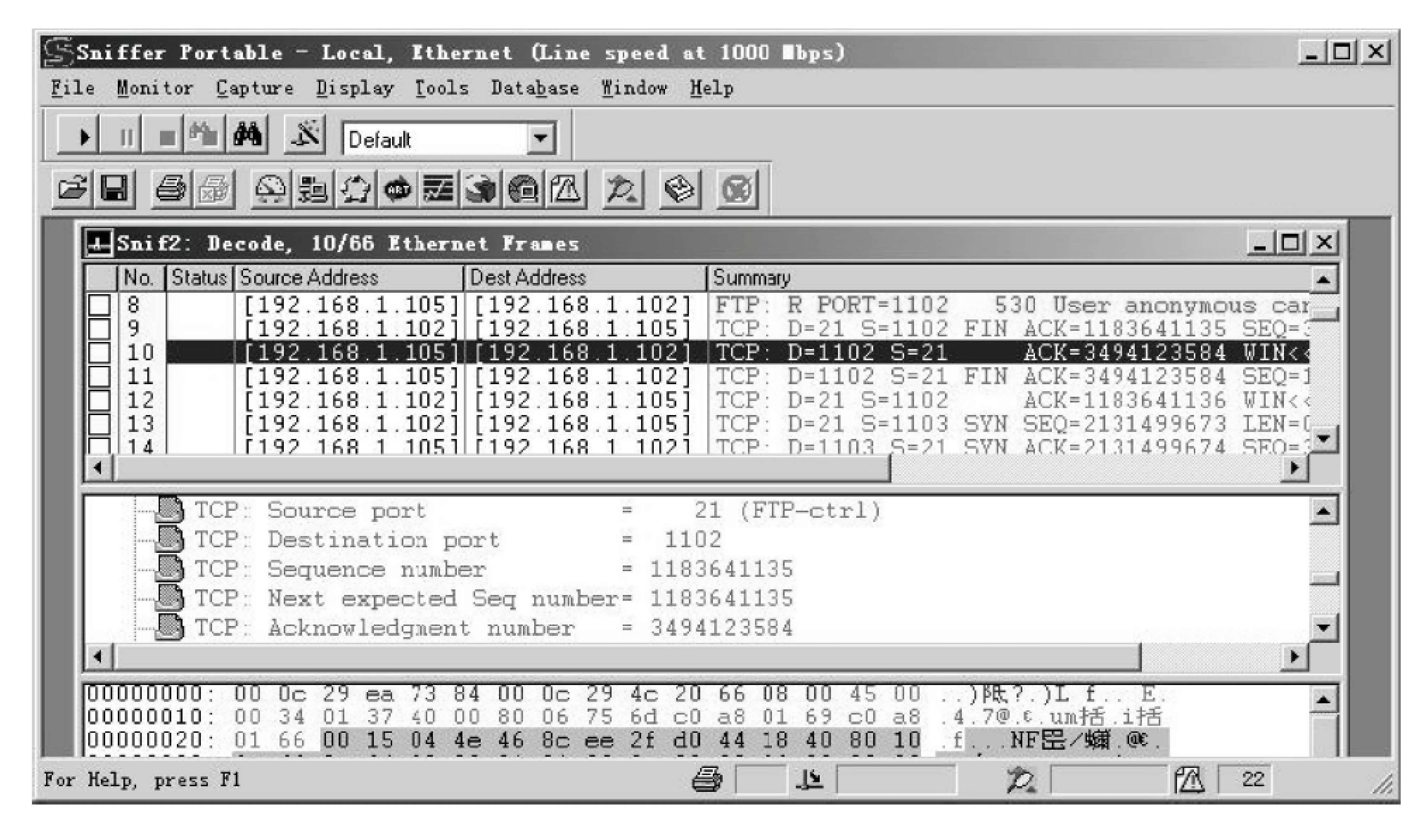


图 9.15　第 2 条 FIN 消息

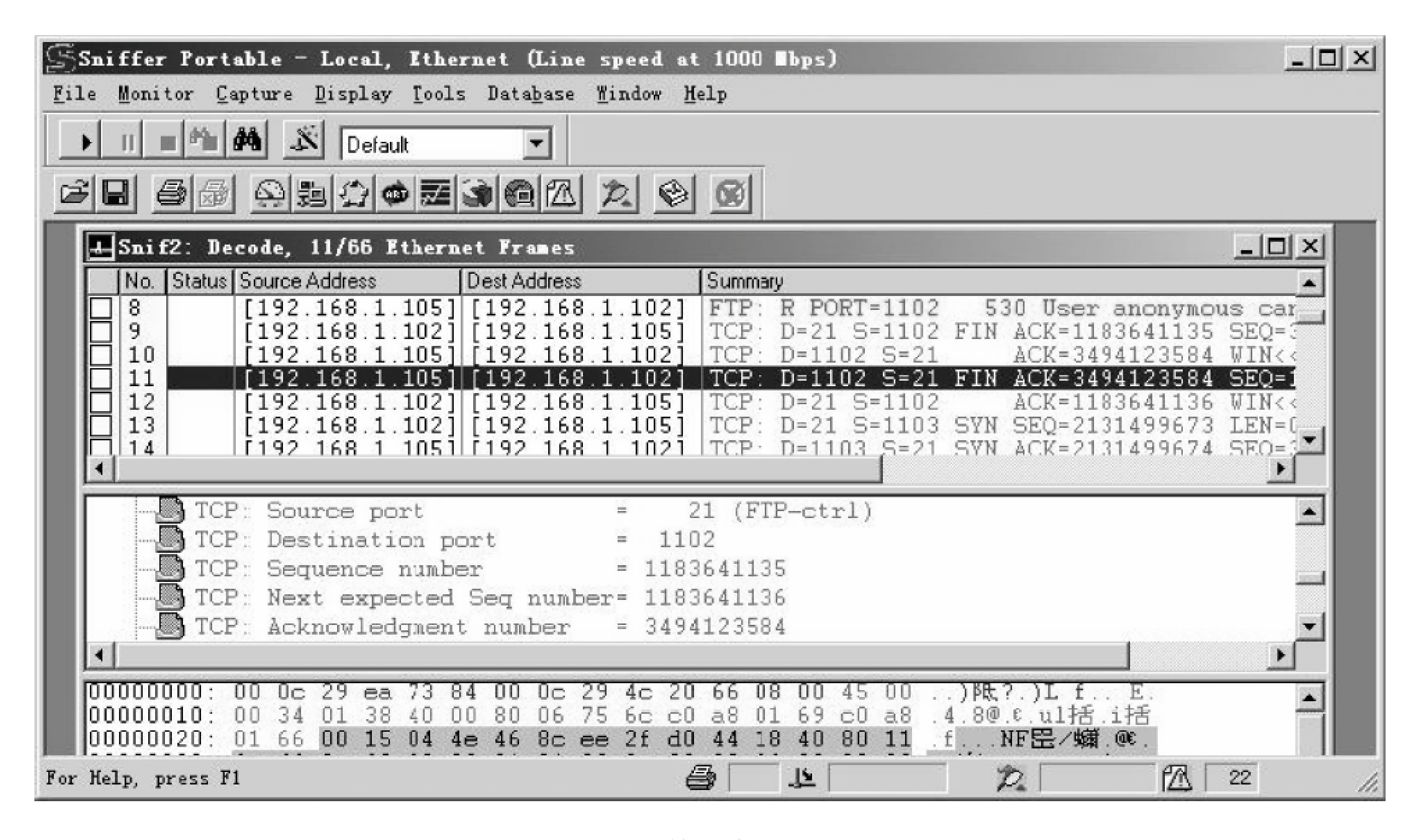


图 9.16　第 3 条 FIN 消息

如图 9.18 所示，从第 4 条到第 8 条数据包显示了 FTP 客户机使用匿名账号登录 FTP 服务器的一个过程，其中第 7 条消息显示了匿名账号的密码为 111。第 8 条消息说明该匿名登录过程被服务器拒绝了。

如图 9.19 所示，从第 28 条到 32 条消息显示了 FTP 客户机使用账号登录 FTP 服务器的一个过程。其中第 29 条消息说明这次登录得用户名为 user1，第 31 条消息说明这次登录的密码为 111，第 32 条消息显示登录成功。

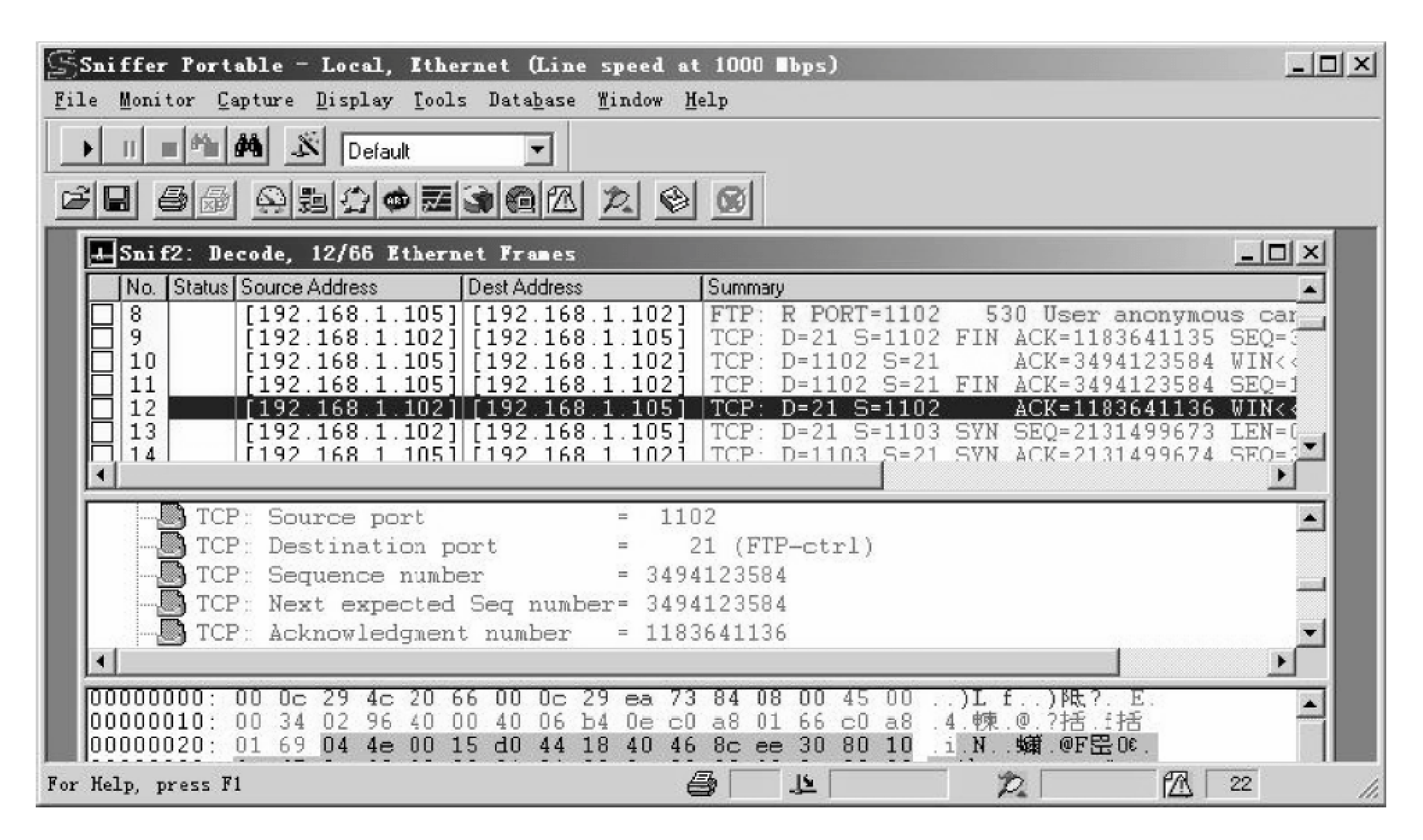


图 9.17 第 4 条 FIN 消息

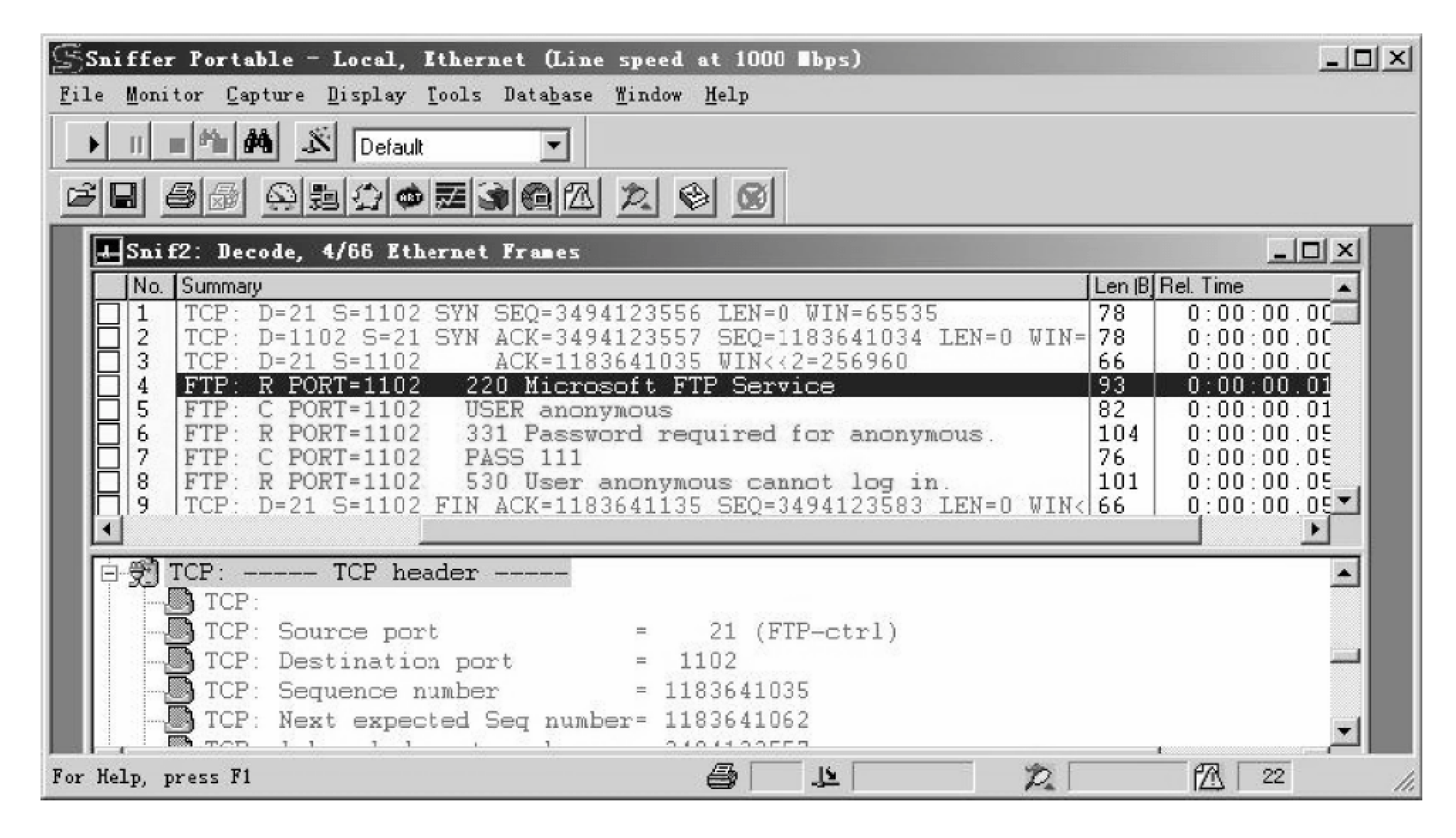


图 9.18 FTP 的匿名登录过程

从以上的分析可以看出，FTP 客户机在登录服务器时，其用户名和密码均是以明文的方式传递的。

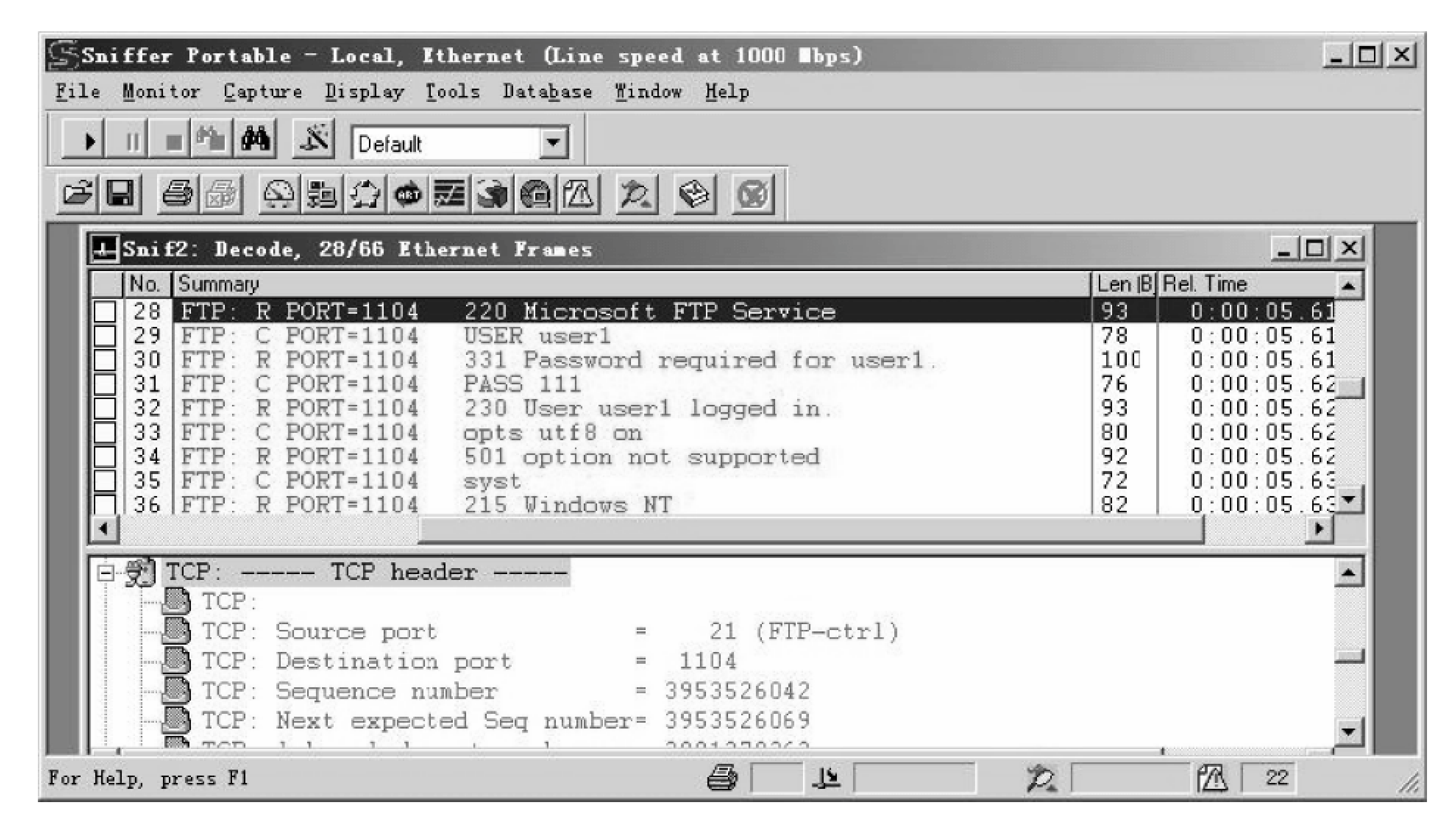


图 9.19 使用账号 user1 登录 FTP 服务器

9.6 实验思考

（1）申请一个 163 的邮箱账号，用 Sniffer 工具抓取登录 163 邮箱时的数据，观察能否找到用户名和密码。

（2）如何利用 Sniffer 工具发现局域网中存在蠕虫病毒的计算机。

实验10 Outlook Express 安全电子邮件

10.1 实验目的与要求

- 理解 Outlook Express 的概念。
- 掌握邮件加密与邮件签名的概念。
- 掌握如何使用 Outlook Express 发送安全电子邮件。

10.2 实验环境

- Window 2000 Server 作为证书颁发服务器。
- Window XP 作为申请电子邮件保护证书的客户机。

10.3 预备知识

Outlook Express 是 Microsoft 公司主打的一款基于 NNTP 协议(Network News Transport Protocol)的电子邮件客户端软件,简称 OE。该软件与 Windows 操作系统软件以及 Internet Explore 网页浏览器绑定在一起,可以认为是一款免费软件。

Outlook Express 客户端软件是采用 POP3/SMTP 协议来完成电子邮件的收发的。其中 POP3 协议(Post Office Protocol 3)为邮局协议的第 3 版本,它规定如何将个人电脑与预定义的 POP3 邮件服务器进行通信,以下载邮件服务器上的电子邮件。SMTP(Simple Mail Transfer Protocol),为简单电子邮件传输协议,它规定了如何将个人电脑上的电子邮件发送到预定义的 SMTP 邮件服务器上,再通过该服务器将邮件再转发到收件人的邮件服务器上。

Outlook Express 除了具有电子邮件收发和通信录管理等邮件客户端的基本功能外,还支持安全电子邮件,即具备对邮件进行加密与数字签名的功能。若要使用 Outlook Express 中的安全电子邮件,使用者需要数字标识。

1. 获取数字标识

数字标识即数字证书,它采用公钥体制,即利用一对互相匹配的密

钥进行加密、解密，提供在计算机世界里验证实体身份的手段。数字标识由一个公众信任的可信机构（一般为数字证书认证中心 CA，Certificate Authority）产生，该机构将一个实体（如一个用户）的真实身份和他的公钥通过一种可公开验证的、可信的方式绑定在一起，形成一个证明该实体身份的数字标识。该机构不仅负责数字标识的公开颁发，而且还采用技术手段和安全策略不断验证数字标识的有效性。目前全球最大的商业性的数字标识提供商是 Verisign 公司（www. Verisign. com），其他较为著名的提供商有 ThawteConsulting（www. thawte. com）、BankGateCA（www. bankgate. com）等。国内目前较为著名的区域性的数字标识的提供商有上海数字证书认证中心（www. sheca. com）、北京数字证书认证中心（www. bjca. org. cn）、山东省数字证书认证管理有限公司（www. sdca. com. cn）等。

2. 安全电子邮件

当拥有数字标识（数字证书）时，用户就可以发送安全电子邮件了。Outlook Express 可以使用数字签名和加密对在 Internet 中传输的电子邮件进行保护。当用户使用自己的数字签名时，则可以对电子邮件进行签名，这样接收方能够确认该用户是邮件正确的发送方，并且确认邮件在传输过程中未被篡改。当用户使用别人的数字标识时，则可以对电子邮件进行加密，这样只有正确的接收方可以解密邮件内容。对同一封电子邮件，可以同时使用加密和签名来保护。

Outlook Express 使用标准 S/MIME（Secure/Multipurpose Internet Mail Extensions，安全多功能互联网邮件扩展），任何人能够用支持该技术的程序阅读安全电子邮件。同样，也可以用支持 S/MIME 技术的电子邮件程序阅读他人撰写的邮件。Outlook Express 具有内置安全电子邮件功能，可以提供如下服务。

- 发送签名的邮件　签名电子邮件允许收件人验证发送者的身份。
- 接收签名的邮件　邮件接收者可以验证已签名邮件的发送者的身份——该邮件是否由指定用户发送、在发送过程中是否已更改。已签名的邮件带有特定的已签名图标。如果接收到的已签名邮件出现问题，则表明该邮件已被更改或来自其他发送人。
- 发送加密的邮件　将电子邮件加密会防止传输过程中邮件内容被泄密。要将电子邮件加密，发送者需要有收件人的数字标识。需要注意的是，收件人的电子邮件账号应该与“通讯簿”中收件人的数字标识具有对应关系。
- 接收加密的邮件　当收到加密的电子邮件信息时，若收件人是加密邮件的正确接收者，那么 Outlook Express 会自动将电子邮件解密。
- 数字标识的传播　当用户 A 需要接收其他用户发给他的加密邮件前，A 需要先将自己的数字标识发送给其他用户。此时，A 只需要给这些用户发送签名电子邮件即可，Outlook Express 会自动在邮件中包含用户 A 的数字标识。另外，其他用户还可以利用 Outlook Express 提供的目录服务功能来检索用户 A 的数字标识，并将该标识添加到自己的“通讯簿”中。
- 更改数字标识的可信状态　当将某人的数字标识添加到通讯簿中时，与之相关的信任状态表明“通讯簿”的拥有者是否信任该数字标识。如果某数字标识的所有者发出警告，怀疑数字标识私人密钥已受到损害，那么“通讯簿”的拥有者就可能将信任

状态更改为“明确不信任”。

3. Outlook Express 与 Outlook 的区别

Outlook Express 不是 Microsoft Office 的产品，它是 Microsoft Internet Explorer 中包含的提供基本功能的电子邮件程序。该程序为免费程序，并且该程序可以帮助用户完成发送和接收邮件等基本工作。

Outlook 是 Microsoft Office 产品中的一个组件，能够在安装 Office 时自动安装。Outlook 是一个集成的桌面信息管理程序，可以帮助管理邮件、约会、联系人和任务，也可以跟踪活动、打开和查看文档及共享信息。使用 Outlook，可以轻松完成下列工作。

- 不仅可以跟踪活动，而且可以管理个人和商务信息，如电子邮件、约会、联系人、任务和文件。
- 通过使用电子邮件、小组日程安排、公用文件夹等可以与小组共享信息。
- 与其他 Office 程序共享信息，并从 Outlook 内部浏览和查找 Office 文件。
- 通过连接到 WWW 以共享信息。
- 如果是开发者，还可使用编程选项来自定义 Outlook。

表 10.1 给出了 Outlook express 与 Outlook 的区别。

表 10.1　Outlook express 与 Outlook 的区别

功　　能	Outlook Express	Outlook
发送和接收电子邮件	√	√
支持 IMAP、HTTP 和 POP Internet 电子邮件服务器	√	√
支持 Microsoft Exchange Server		√
通讯簿和联系人文件夹	√	√
支持多个通讯簿		√
支持完全集成的日历功能		√
“任务”文件夹		√
垃圾邮件过滤		√
“便笺”文件夹		√
支持新闻组	√	
签名和信纸	√	√
电子邮件安全	√	√

10.4　实验内容

本章的实验内容主要包括以下 4 部分：

(1) 演示如何申请用于在 Outlook Express 中保护电子邮件的数字证书。

(2) 演示证书服务器端如何签发数字证书。

(3) 演示如何在客户端的计算机上安装数字证书。

(4) 演示如何设置 Outlook Express，以便能够利用数字证书对电子邮件进行保护。

10.5 实验步骤

10.5.1 申请电子邮件保护证书

在 Windows 2000 操作系统上打开浏览器，输入证书颁发服务器的地址：http://192.168.1.100/certsrv，如图 10.1 所示。

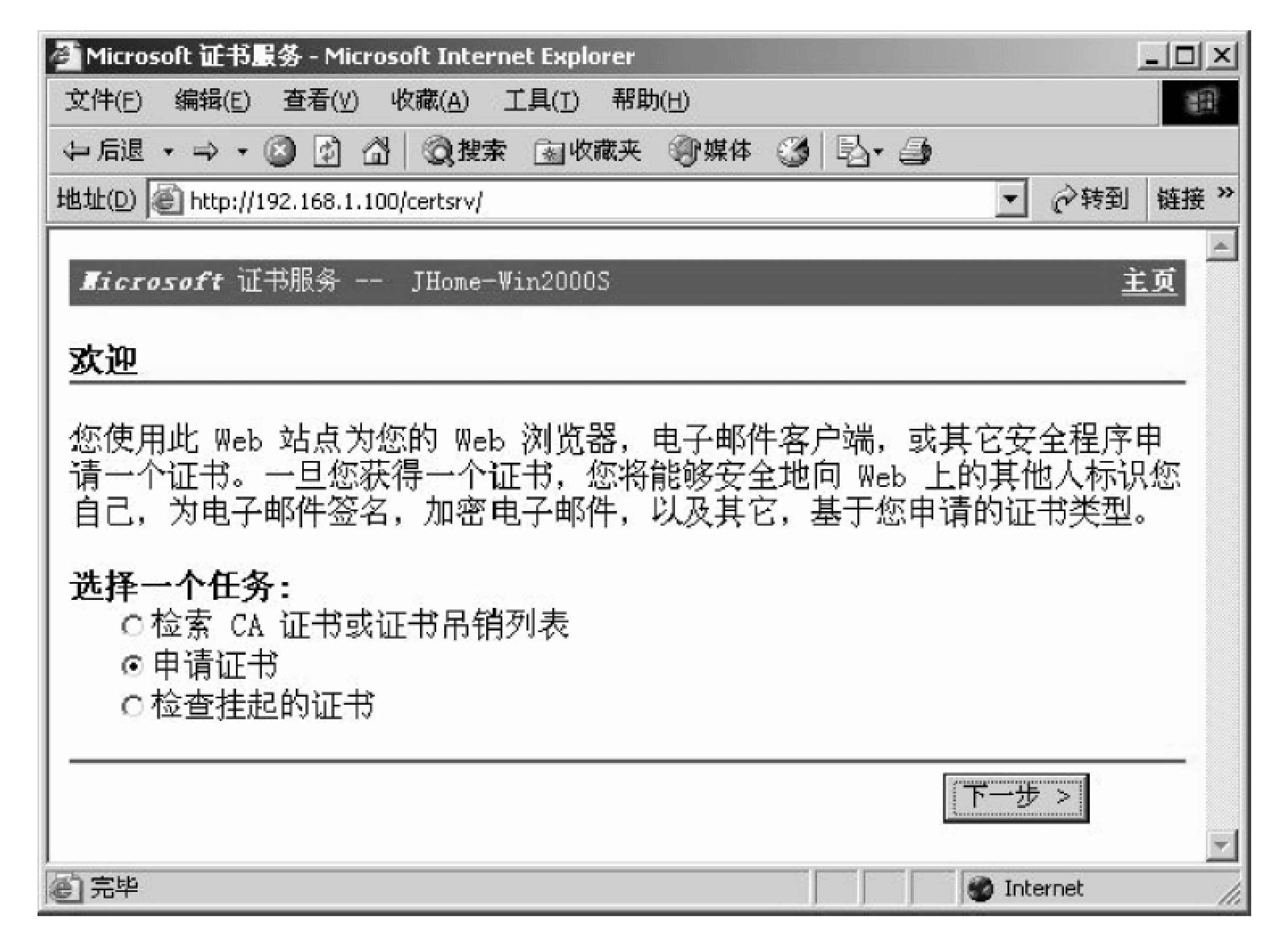


图 10.1 证书申请页面

选择"申请证书"，然后单击"下一步"按钮。在出现的"电子邮件保护证书-标识信息"页面中单击"更多选项"，在出现的内容中单击"高级证书申请"。然后在"需要的证书类型"中选择"电子邮件保护证书"，并选中"标记密钥为可导出"复选框，如图 10.2 所示。

在该页面的上部输入用户名、邮件地址等相关信息，其中名称为 sdfi_user1，电子邮件地址为 sdfi_user1@163.com。如图 10.3 所示，然后单击"提交"按钮。

此时会弹出一个标题为"潜在的脚本冲突"对话框，如图 10.4 所示，提示用户确认是否在当前的网站上申请证书，若确认，则单击"是(Y)"按钮。

至此完成了证书的申请工作。

10.5.2 证书的颁发

Windows 2000 Server 证书服务器的管理员依次单击"开始"→"程序"→"管理工具"→"证书颁发机构"命令，打开"证书颁发机构"管理器，如图 10.5 所示。

单击域名前的加号，选择"待定申请"，在窗口右侧找到刚刚申请的电子邮件保护证书。右击该证书，在弹出的快捷菜单中依次选择"所有任务"→"颁发"，将该证书颁发，如图 10.6 所示。

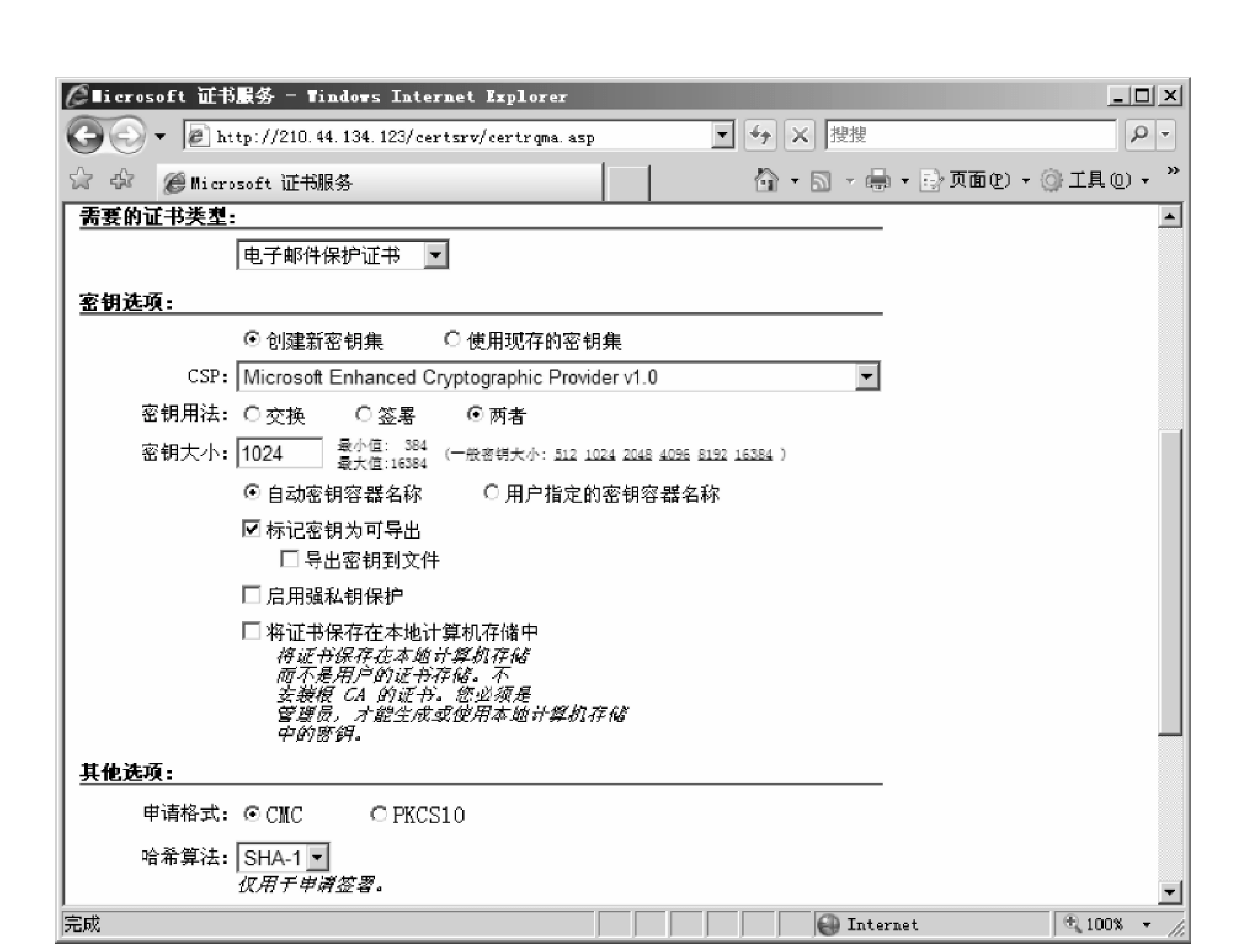


图 10.2 设置密钥选项

Microsoft 证书服务 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹 媒体
地址(D) http://192.168.1.100/certsrv/certrqbi.asp?type=1 转到 链接

请输入将在您的证书中出现的标识信息:

名称: user_1
电子邮件: user_1@jhome.com
公司: Home
部门: Computer
城市: Jinan
省: Shandong
国家(地区): CN

更多选项 >>

提交 >

完毕 Internet
开始 Microsoft 证书服务 - Micr... 14:54

图 10.3 填写相关信息



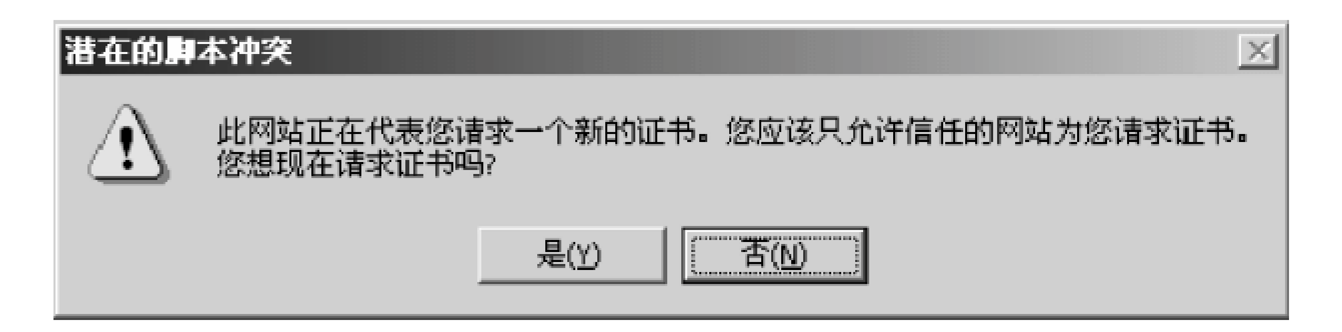


图 10.4 申请证书时的警告信息

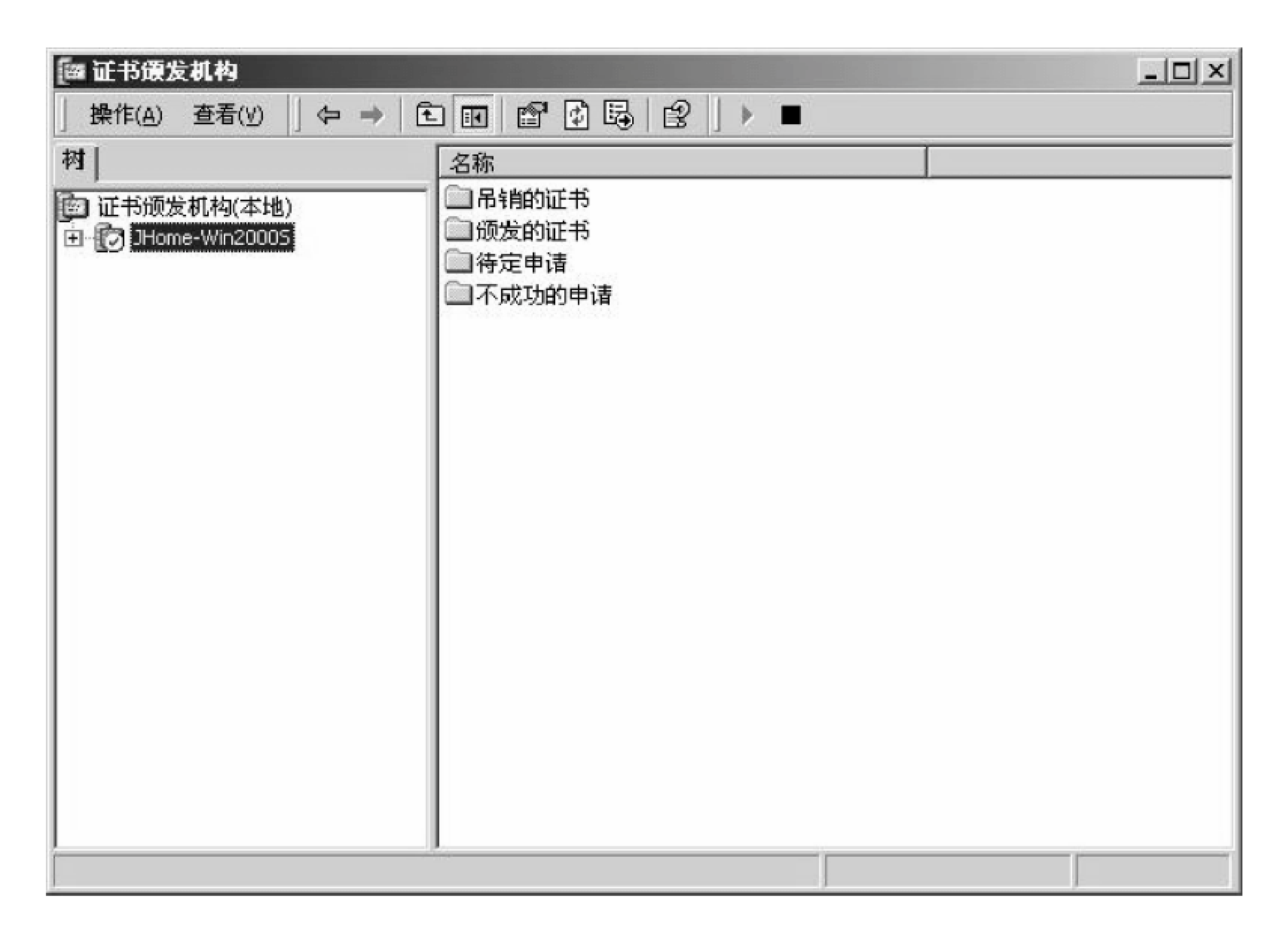


图 10.5 证书颁发机构



图 10.6 颁发证书

10.5.3 下载并在客户机中安装证书

切换到 Windows 2000 操作系统，在浏览器地址栏中重新输入证书颁发服务器的地址：http://192.168.1.100/certsrv，在出现的页面中选择“检查挂起的证书”，如图 10.7 所示，然后单击“下一步”按钮。

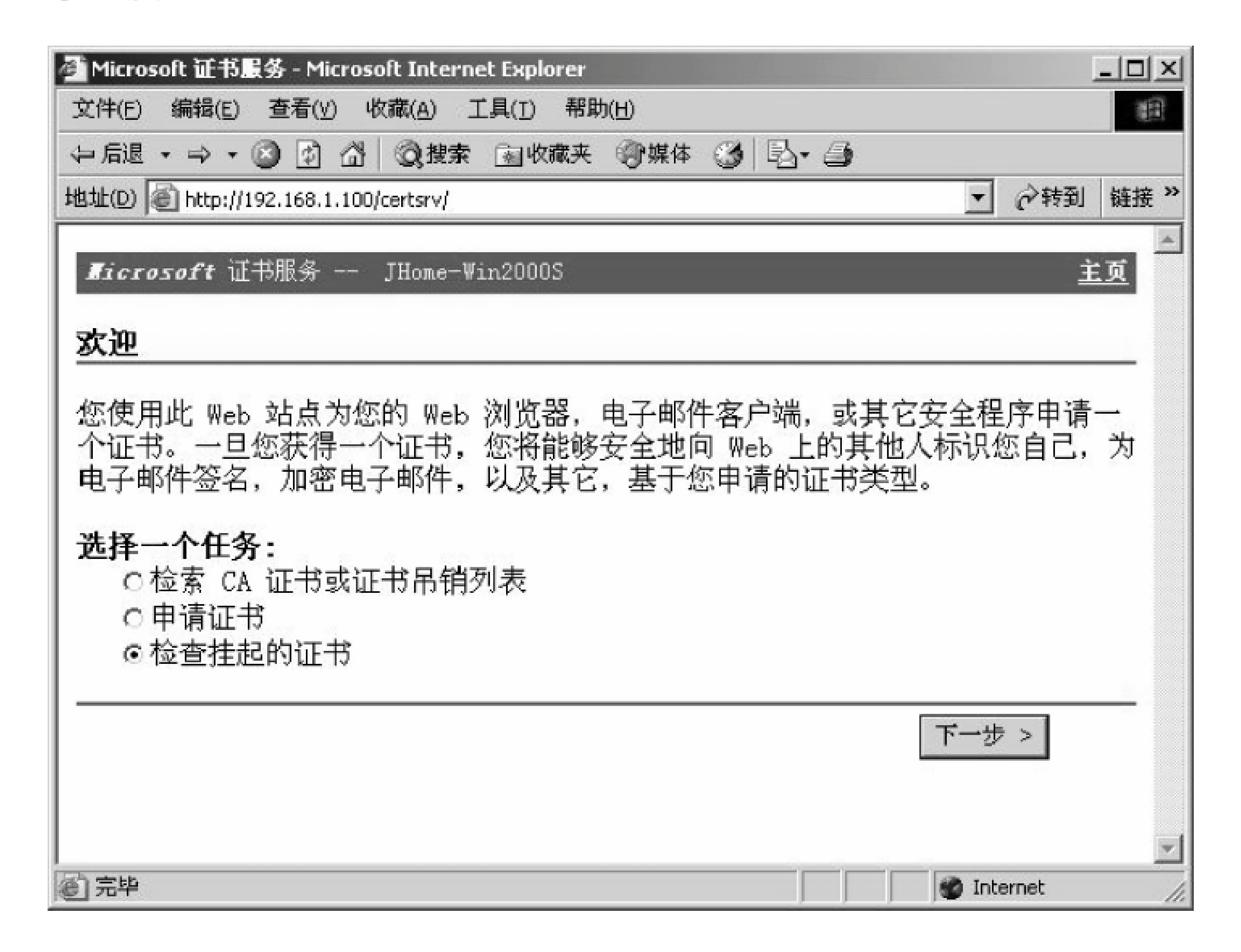


图 10.7 检查挂起的证书

在出现的页面中直接单击“下一步”按钮，如图 10.8 所示。

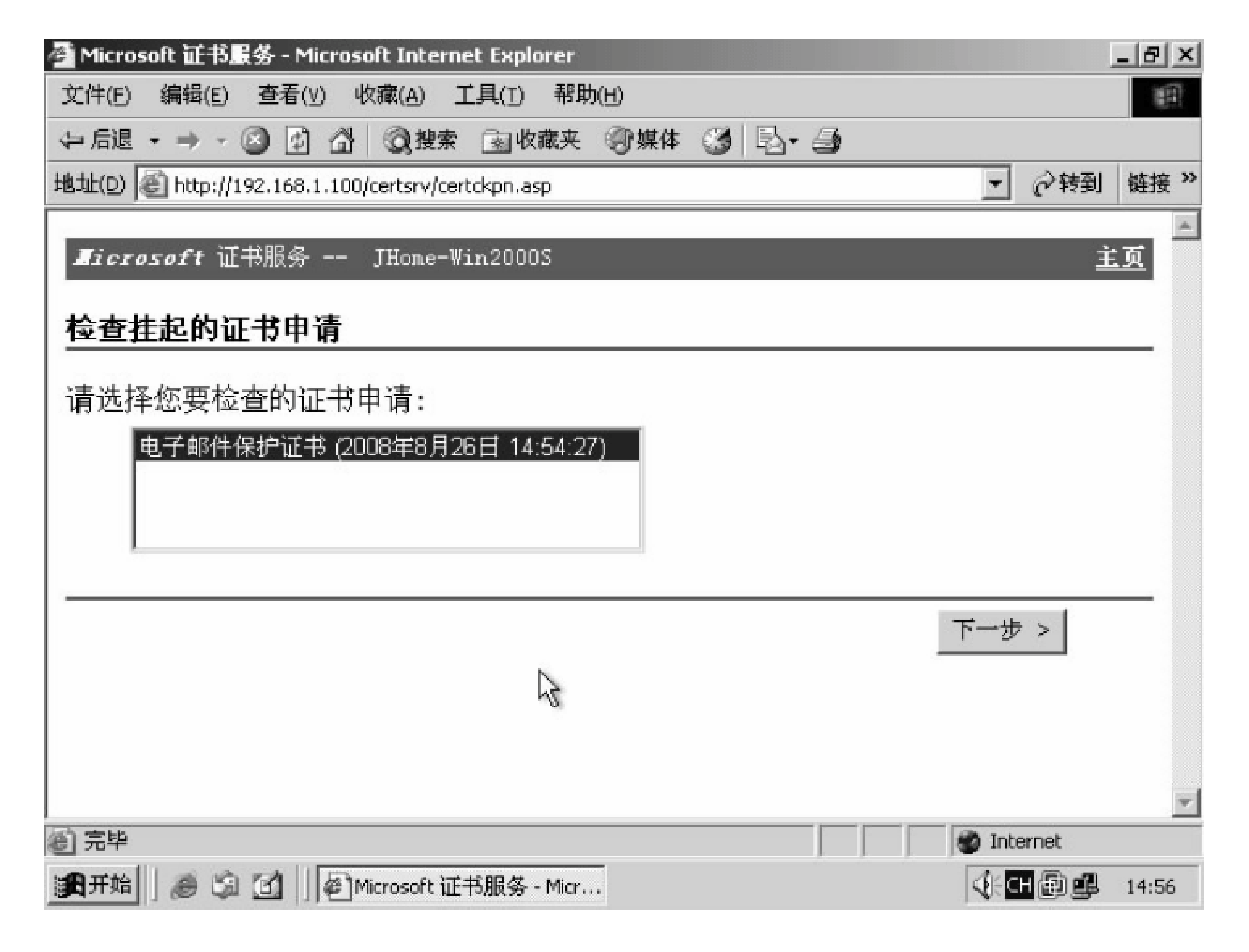


图 10.8 选择要安装的证书

在出现的页面中单击“安装此证书”，在弹出的“潜在的脚本冲突”对话框中单击“是(Y)”按钮，将证书安装到浏览器中。

单击浏览器的“工具”下拉菜单，然后选择“Internet 选项”命令，在弹出的“Internet 选项”对话框中选择“内容”选项卡，如图 10.9 所示。



图 10.9 “Internet 选项”对话框

在图 10.9 中单击“证书”，在弹出的“证书”对话框中选择“个人”选项卡，并找到刚刚安装的证书，如图 10.10 所示。



图 10.10 选择电子邮件保护证书

单击图 10.10 中对话框下面的“导出”按钮，进入“证书导出向导”对话框。单击“下一步”按钮，在出现的页面中选择“是，导出私钥”按钮，然后按照提示信息，将带私钥的证书导

出到一个名为 sdfi_user1.pfx 的证书文件中(该文件包含公钥和私钥)。同时再实施一次该证书的导出,在此次导出中选择不导出私钥,并将导出的证书保存在一个名为 sdfi_user.cert 的文件中(该文件只含公钥,不含私钥)。

按照同样的方式再申请一个邮件保护证书,其用户名为 sdfi_user2,邮件地址为 sdfi_user2@163.com,并将证书从浏览器中导出到一个名为 sdfi_user2.pfx 的证书文件和一个明文 sdfi_user2.cert 的证书文件中。

为了保证两个证书安装在别的客户机上也能使用,还必须将 CA 的公钥证书下载下来,方法如下。

浏览器地址栏中重新输入证书颁发服务器的地址:http://192.168.1.100/certsrv,在出现的页面中选择"检索 CA 证书或证书撤销列表",单击"下一步"按钮,在出现的新页面中单击"下载 CA 证书",将该 CA 证书以文件的形式保存在硬盘上,如图 10.11 所示。

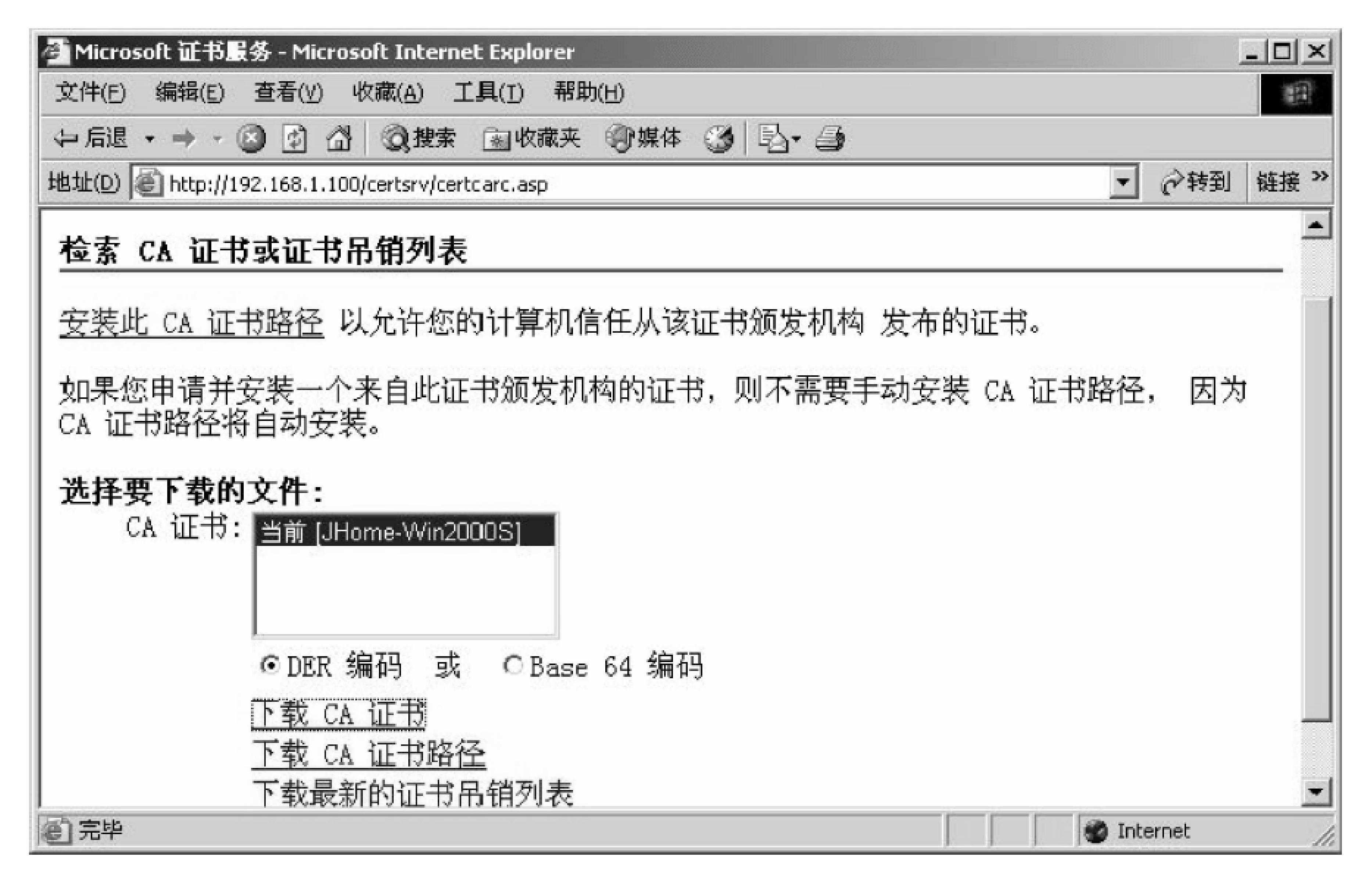


图 10.11 下载 CA 证书

10.5.4 配置 Outlook Express

假设现在名为 sdfi_user1 的用户打算使用 Outlook Express 发送安全的电子邮件给用户 sdfi_user2,那么 sdfi_user1 首先在自己的机器上安装 CA 证书,然后双击 sdfi_user1.pfx 文件,将它作为自己的证书安装在机器的证书管理器中,最后安装用户 sdfi_user2 的公钥证书 sdfiuser2.cert。该过程结束后,sdfi_user1 的证书将出现在证书管理器的"个人"选项卡中,而 sdfi_user2 的证书将出现在"其他人"选项卡中,如图 10.12 和图 10.13 所示。

1. 配制 Outlook Express 账户

打开 Outlook Express 客户端,在"工具"下拉菜单中单击"账户",打开"Internet 账户"对话框。然后单击该对话框右侧的"添加"→"邮件"(如图 10.14 所示),打开"Internet 连接

图 10.12　sdfi_user1 的证书



图 10.13　sdfi_user2 的证书

向导”，为 Outlook Express 添加账户，如图 10.15 所示。

2. 设置签名证书

打开“Internet 账户”对话框，选择“邮件”选项卡，然后单击右侧的“属性”按钮，弹出“pop.163.com 属性”对话框，如图 10.16 所示。

单击该属性框中签署证书栏的“选择”按钮，将 sdfi_user1 的证书添加进来。如图 10.17 所示：

单击“pop.163.com”对话框下方的“确定”按钮，完成签署证书的安装工作。

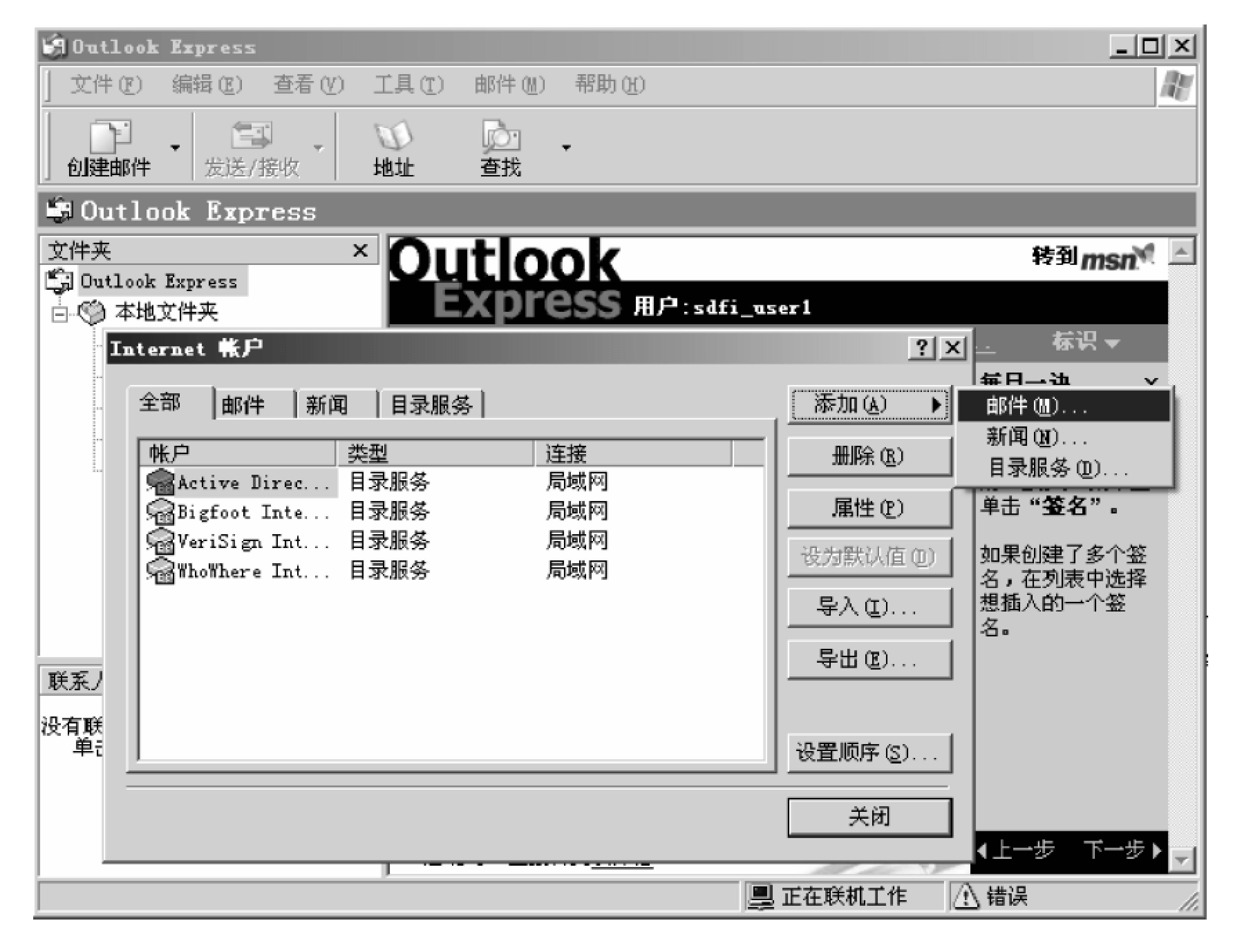


图 10.14 添加新账号

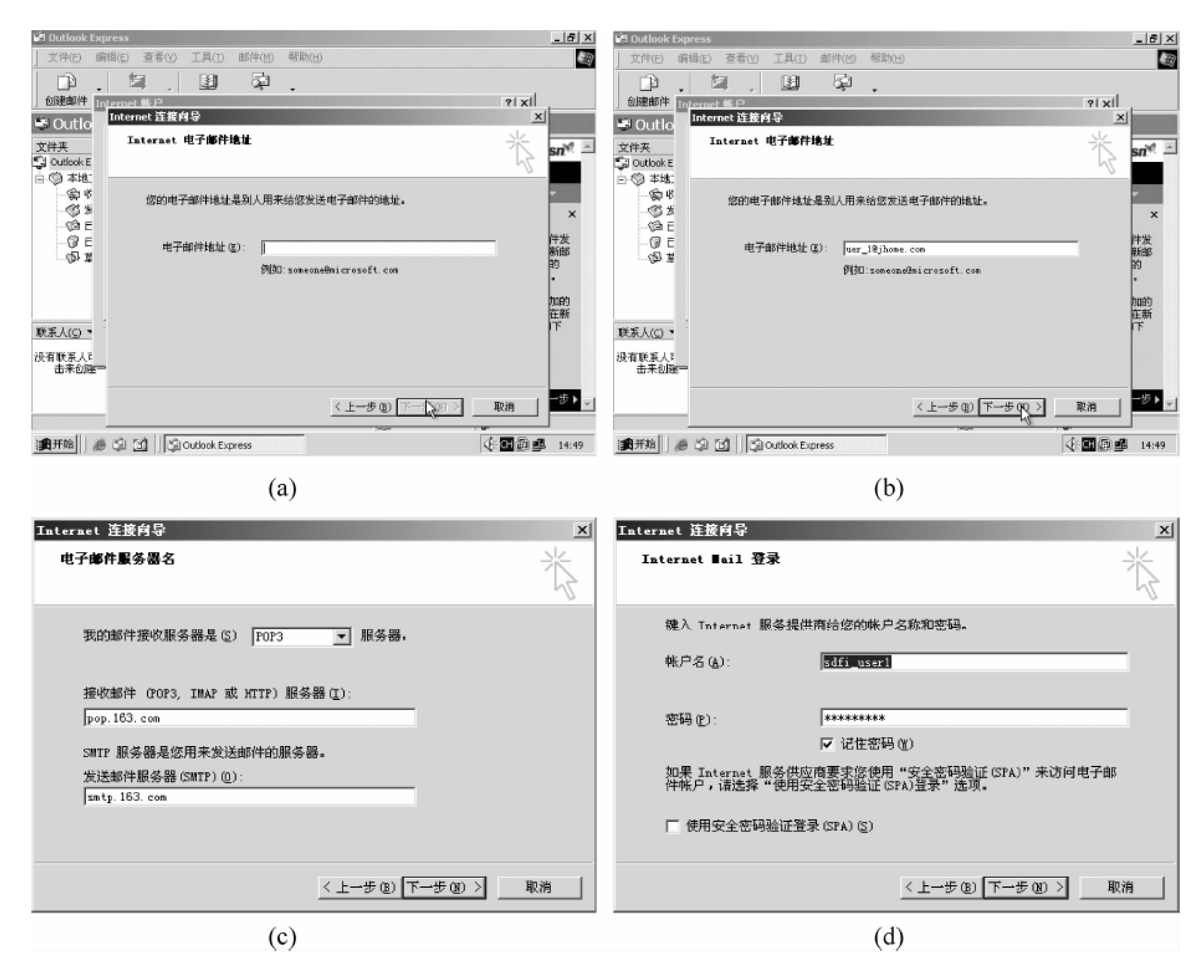


图 10.15 配置账号



图 10.16　设置账户属性

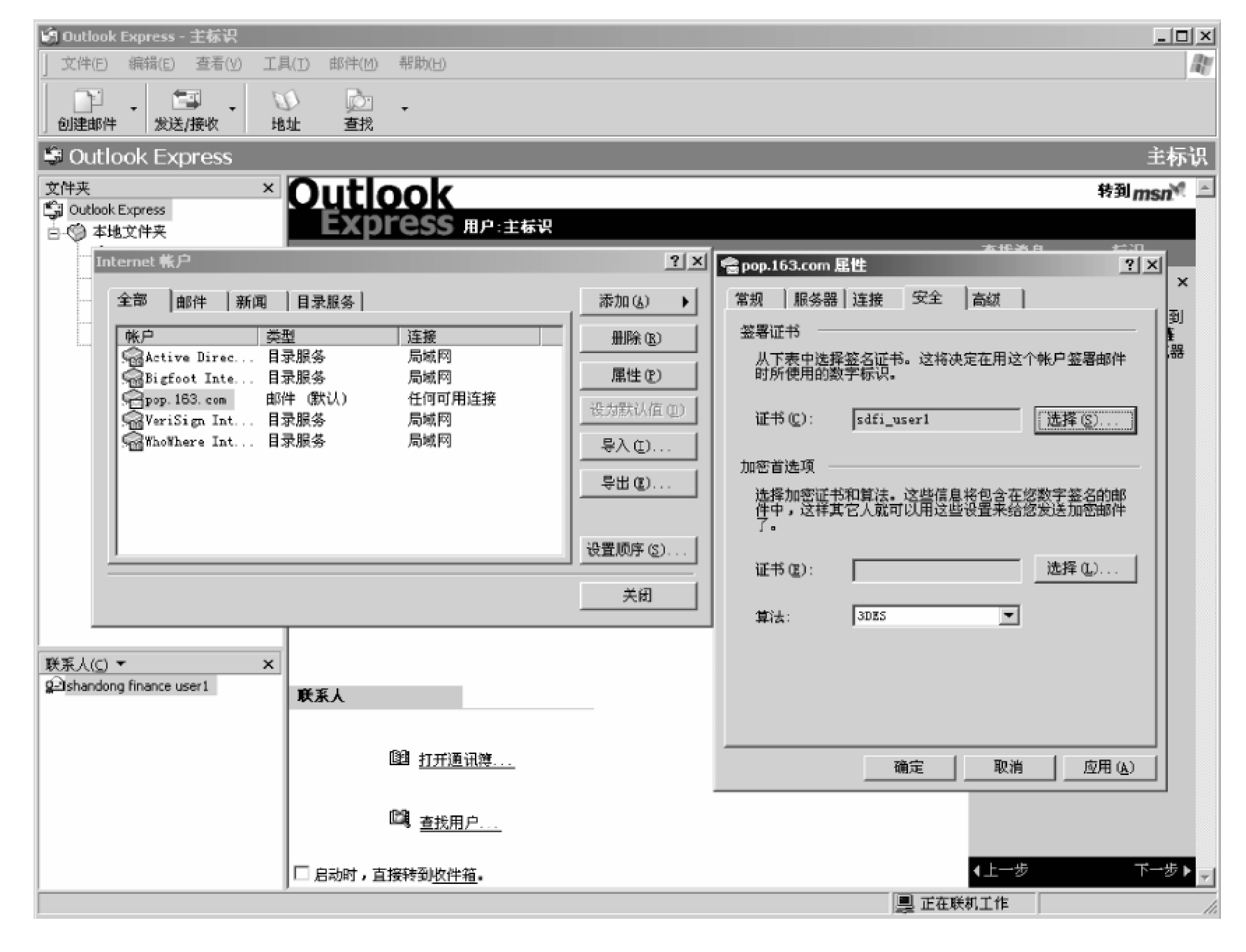


图 10.17　添加签署证书

3. 添加加密证书

在 Outlook Express 客户端的左下方单击“联系人”，打开添加联系人的“属性”对话框。

在“姓名”属性页中填入相关信息,在填入电子邮件后,单击右侧的“添加”按钮,完成电子邮件的添加。然后选择“数字标识”选项卡,单击右下方的“导入”按钮,在磁盘上将名为 sdfi_user2. cert 的证书导入进来,如图 10.18 所示。

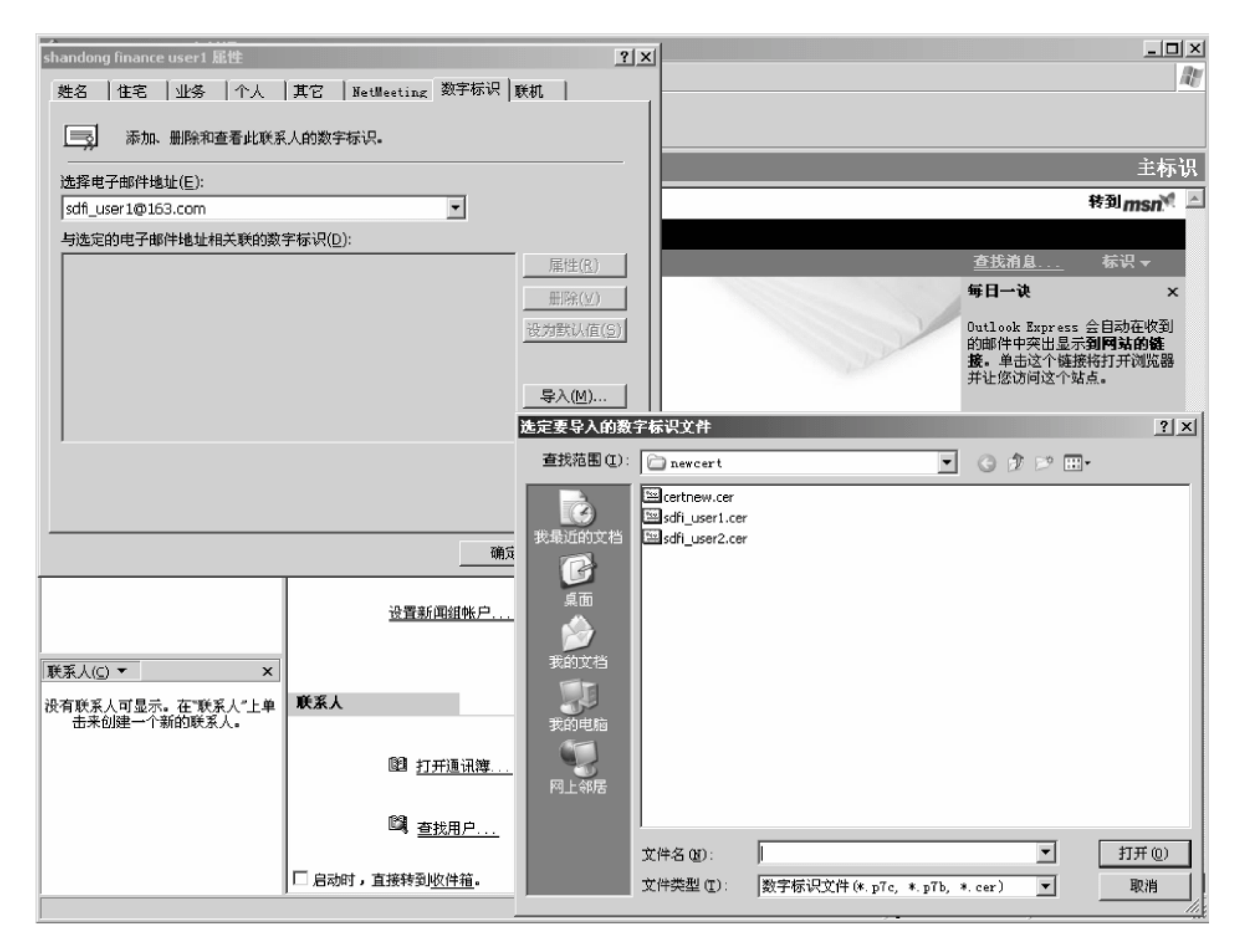


图 10.18 添加加密证书

当导入成功后,将显示如图 10.19 所示的对话框。



图 10.19 加密证书添加成功

此时,签署证书和加密证书的安装工作完成了,用户 sdfi_user1 就可以对用户 sdfi_user2 发送签名加密电子邮件了。其中签名功能使用的是 sdfi_user1 自己证书的私钥来完成,加密功能使用的是 sfdi_user2 证书中的公钥来完成。

注:目前我国各大邮件提供商均对免费邮件的 POP3/SMTP 服务设置了限制,只有等级较高的邮件账户才能享用该服务,而新注册的账户一般不能使用该服务。

10.6 实验思考

(1) 在申请数字证书时,若选择的证书类型不是"电子邮件保护证书",那么该证书能否用于 Outlook Express 中的邮件保护,请通过实验检验。

(2) 若申请数字证书时,所填写的电子邮件地址与发信人的电子邮件地址不一致,那么该证书能否保护该发信人的电子邮件,请通过实验检验。



实验 11 SSH 安全连接

11.1 实验目的与要求

- 理解 SSH 的基本概念和原理。
- 掌握如何使用 SSH 来保护信息安全。

11.2 实验环境

- Windows 2003 安装 F-Secure SSH 服务器端。
- Windows XP 安装 F-Secure SSH 客户端。

11.3 预备知识

传统的网络服务协议在设计之初主要考虑协议的功能性,而对安全性考虑不足。如 FTP、Telnet 等远程登录协议,其登录账户的用户名和口令以及传输的数据均是以明文的方式出现在网络上。使用简单的工具,比如 Sniffer 工具,能够很容易地在网络上获得这些用户名和口令以及明文数据,从而造成信息安全事件。

SSH 是目前较可靠的,专门为远程登录会话以及其他网络服务提供安全性的协议。SSH 的英文全称为 Secure Shell,是 IETF(Internet Engineering Task Force)的 Network Working Group 所制定的一簇协议,其目的是在不安全的网络中提供安全登录以及数据加密等其他安全服务,有效解决数据远程传输过程中的信息安全问题。

SSH 协议框架主要由三部分组成:传输层协议、用户认证协议和连接协议。其中连接协议(The Connection Protocol)处于框架的最上层,在该协议中加密信道被划分为若干个逻辑通道,提供给不同的应用层协议使用,如 FTP、Telnet、Pop 协议等;用户认证协议(The User Authentication Protocol)处于连接协议的下方,主要为服务器提供客户端的身份认证机制;传输层协议(The Transport Layer Protocol)位于用户认证协议的下方,主要提供服务器认证、数据机密性、数据完整性等安全服务。同时 SSH 协议框架还为许多高层的网络安全应用协议提供扩展支持。SSH 协议框架的主要层次部分之间的关系可由图 11.1 来表示。

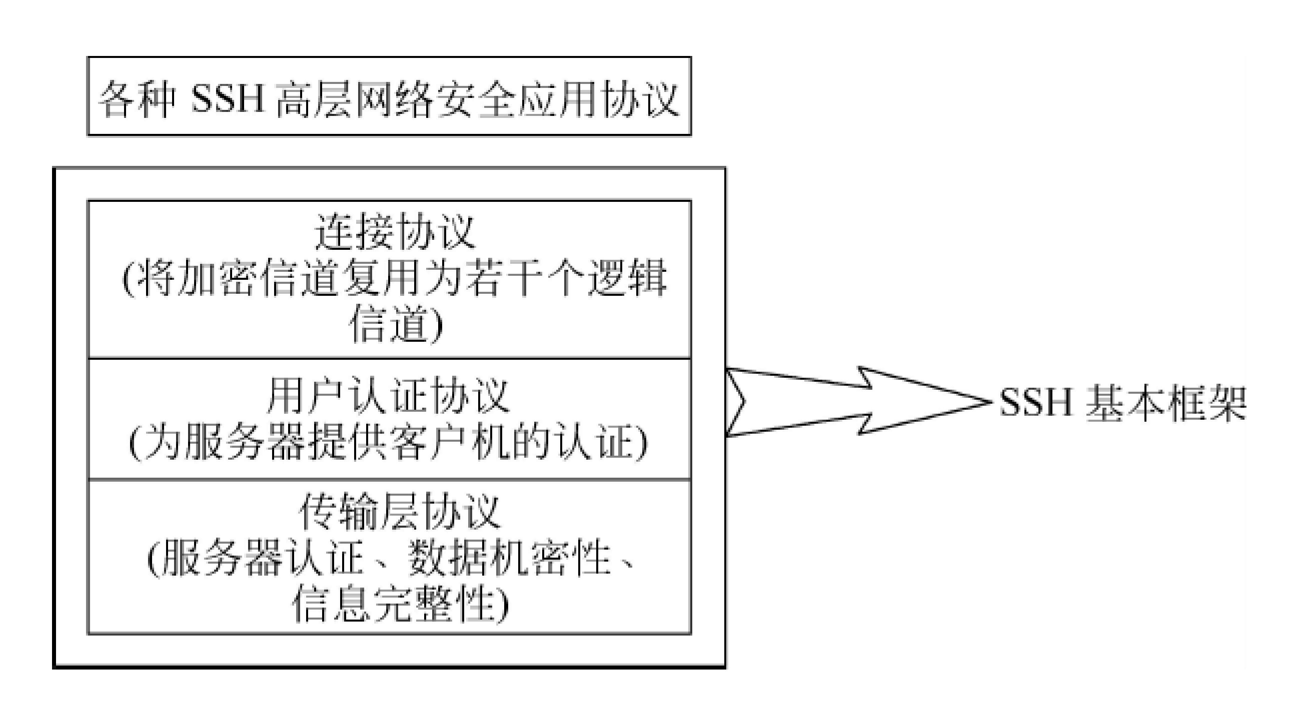


图 11.1　SSH 协议框架的层次结构

SSH 提供了交互式的认证方式，即客户机可以认证服务器，服务器也可以认证客户机，通过认证，双方均可确认对方的真实身份。

11.3.1　服务器认证

远程的服务器可以通过传统的公钥认证或者证书认证来证明自己的身份。在连接初始化时，服务器发送自己的公钥给客户机，若使用证书认证，则公钥会包含在服务器给客户机的证书中。

1. 公钥认证

当使用公钥认证方式来认证服务器时，客户机与服务器的第一次连接最为重要。在第一次的连接中，客户机会收到一个作为服务器标识符的公钥，并给客户机的用户展示该公钥的数字指纹。用户可以通过联系服务器的管理员来分辨该公钥的合法性，当确认该数字指纹的合法性后，用户可以选择在客户机中存储该公钥，以便在以后的连接中用于认证服务器。如果公钥的数字指纹没有被验证通过，这意味着客户机连接的服务器很可能是一个恶意服务器，它正在针对客户机发起“中间人攻击”。

2. 证书认证

证书认证主要用于 SSH 工具的商业版本中。采用证书认证方式的服务器认证是通过 Diffie-Hellman 密钥交换来实现的，其流程如下：

(1) 服务器将自己的数字证书(包含其公钥)发送给客户机。

(2) 由于服务器的证书含有 CA(一个公开可信的认证中心)的私钥签名，客户机可以通过公开的方式获取 CA 的公钥，并用此公钥验证服务器证书的合法性。

(3) 客户机分析服务器证书中是否包含正确的域名信息。

(4) 客户机通过向服务器发送一个“挑战”信息来验证服务器是否具有和证书中的公钥相匹配的私钥。

由于在证书认证方式中有 CA 的介入，客户机可以验证服务器证书的合法性，因此恶意服务器的“中间人攻击”不再有效。

一个合法的服务器证书除了要具有正确的数字签名外，还需要处于“激活”状态，即证书

没有被撤销。在 CA 的架构中,被撤销的证书通过在线证书状态查询(OCSP)或者证书撤销列表(CRL)的形式被公开发布出来,客户机用户可以通过在 LDAP(轻量级目录访问协议)服务器上进行 OCAP 查询或者下载 CRL 来检查服务器证书是否已被撤销。

11.3.2 用户认证

SSH 中的用户认证可以采用很多方法来实现。根据 SSH 的使用者需要的安全级别,这些认证方法既可以单独使用,也可以结合使用。

1. 口令认证

这种认证方式下,用户只需要知道远程登录的用户名及口令,就能利用 SSH 协议完成远程登录服务器,并且客户端与服务器之间传输的数据均是加密的。但是,由于没有提供对服务器的认证机制,因此,恶意服务器可以冒充合法的服务器欺骗客户机,使得客户机连接到恶意服务器上进行数据的收发,从而遭受"中间人"攻击。

2. 基于密钥的认证

这种认证方式下,客户端需要创建一对公钥体制下的密钥对,包括公钥和私钥。其中公钥要通过某种方式传递给服务器,让服务器用该公钥完成对客户端的认证。同时,为了完成客户端对服务器的认证,服务器也需要创建一对公私密钥对,并将公钥以某种形式传递给客户端。为了完成公钥在网络中的传递,SSH 协议提供了两种解决方案。第一种方案中,公钥是在初次使用 SSH 时通过网络传递给对方的,由于这种方案对公钥的保护较弱,因此存在较大安全隐患;第二种方案是借助于数字证书和可信认证中心(CA)完成公钥的传递,这种方案基于 PKI 架构(公钥基础设施架构),能够通过密码学原理和安全的密码协议完成公钥的分发、服务器与客户端的相互认证,因此具有高强度的安全性。

此外,SSH 还提供基于主机的认证方式、Kerberos 认证方式、可插入的认证模块(Pluggable Authentication Module)以及基于 RSA SecurID 的认证方式。

11.4 实验内容

本章的实验内容主要包括以下两部分:

(1) 演示如何配置 SSH 服务器、客户机以及登录账户,使用户以口令认证的方式安全地远程登录服务器。

(2) 演示如何更新服务器上的主密钥,以确保 SSH 应用的安全性。

11.5 实验步骤

11.5.1 如何使用口令访问 SSH 服务器

首先在 Windows 2003 上安装 F-Secure SSH 服务器端程序,在 Windows XP 上安装

F-Secure SSH客户端程序。在 Windows 2003 中创建一个用户账户 user1，供 SSH 客户端访问本服务器使用。在 Windows 2003 的 C 盘中创建一个目录 SSHDirecotory，然后右键单击该目录，在弹出的菜单中选择“属性”→“安全”选项卡，如图 11.2 所示。



图 11.2　“安全”选项卡

单击图 11.2 中的“添加”按钮，在弹出的“选择用户或组”对话框中单击“高级”→“立即查找”，选中“user1”，单击“确定”按钮。如图 11.3 和图 11.4 所示。



图 11.3　“选择用户或组”对话框

在“安全”选项卡中为 user1 设置访问该目录的权限，如图 11.5 所示。

在 Windows 2003 中，依次单击“开始”→“所有程序”→F-Secure SSH→Configuration，打开 F-Secure SSH 服务器端的配置程序对话框 F-Secure SSH Server Configuration，如图 11.6 所示。

在 F-Secure SSH Server Configuration 对话框左边的选项栏中选择 Server Settings 下的 Network。然后在右侧的 Listen Address 配置项中填入服务器的 IP 地址，其他配置项均取默认值，如图 11.7 所示。

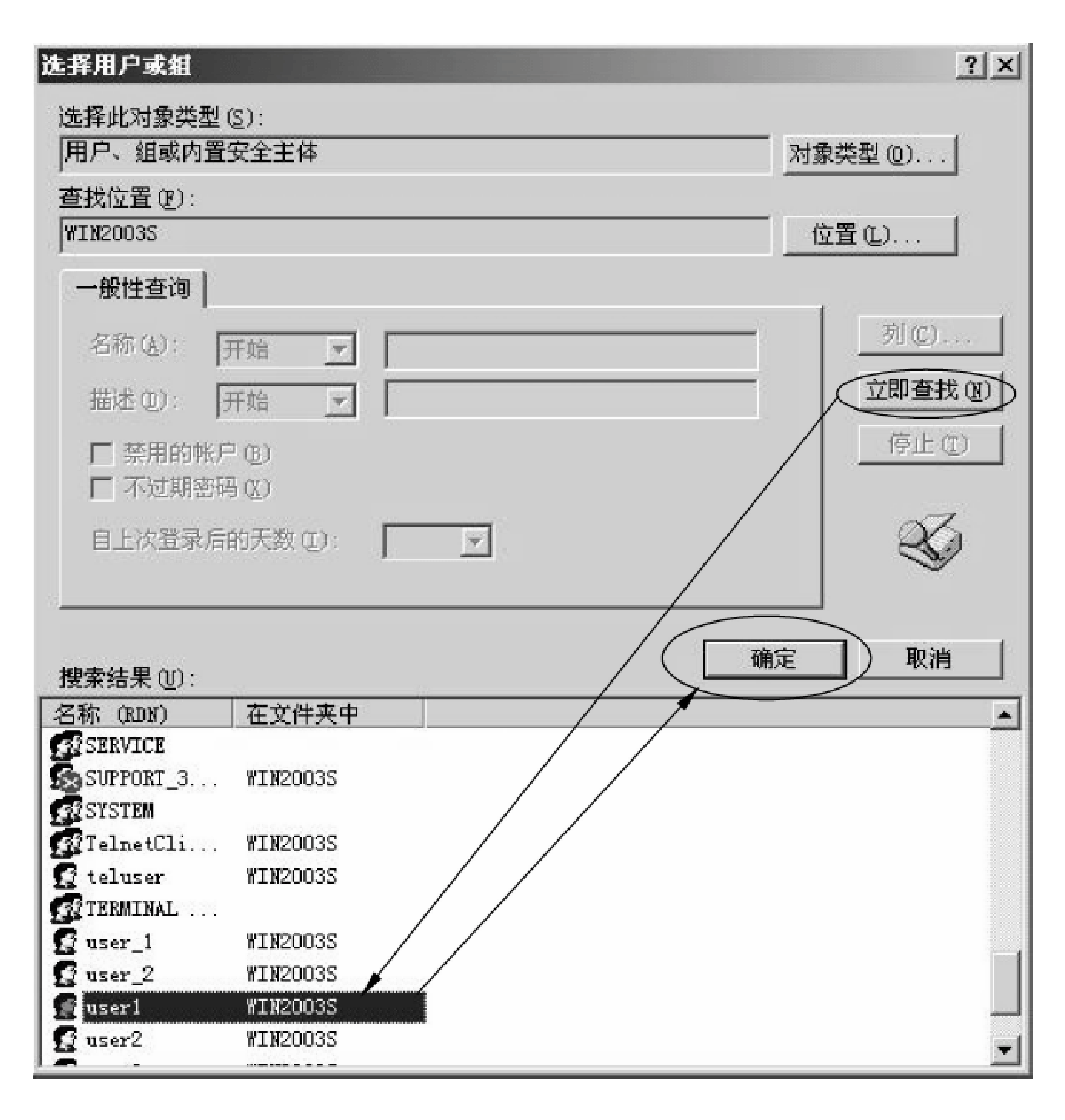


图 11.4 选择 user1

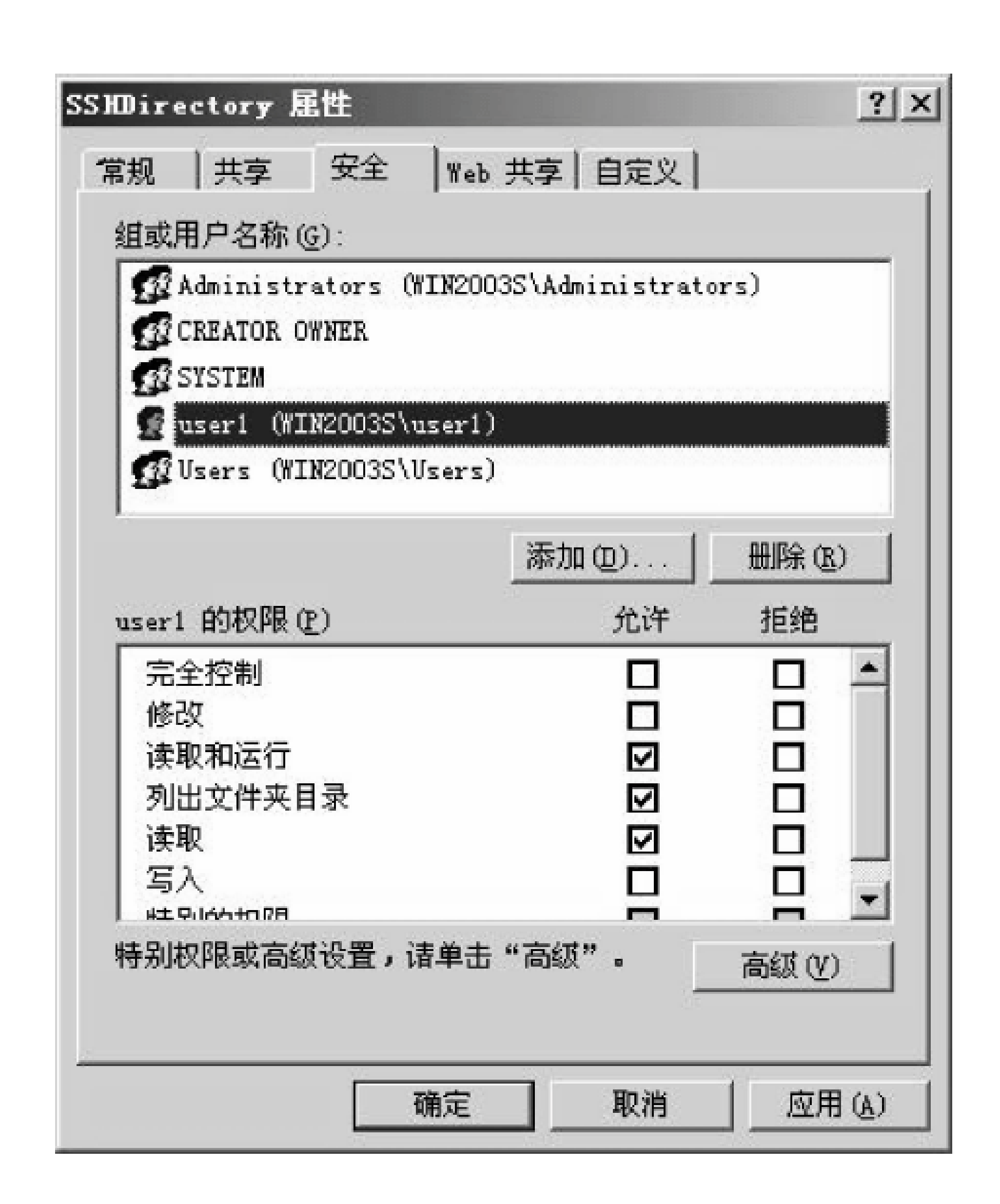


图 11.5 设置 user1 的权限

在 F-Secure SSH Server Configuration 对话框左边的选项栏中选择 SFTP Server，然后在右侧的配置窗口中添加 SSH 服务器的目录供客户端访问。具体操作是，首先单击 Accessible Directories 右侧的“添加”按钮，然后在“HOME=%D”下方出现的空白框中输入

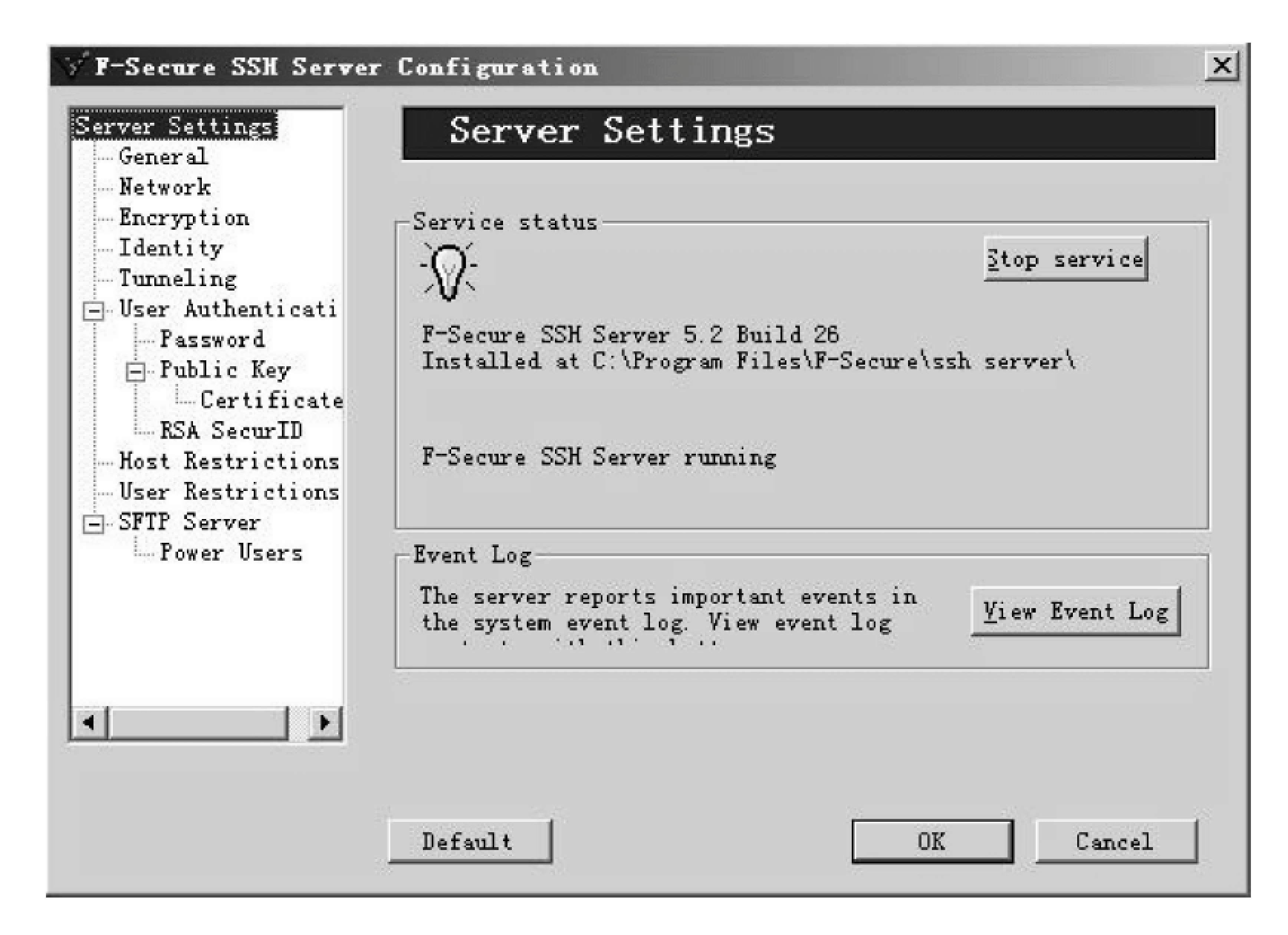


图 11.6　SSH Server 的配置窗口

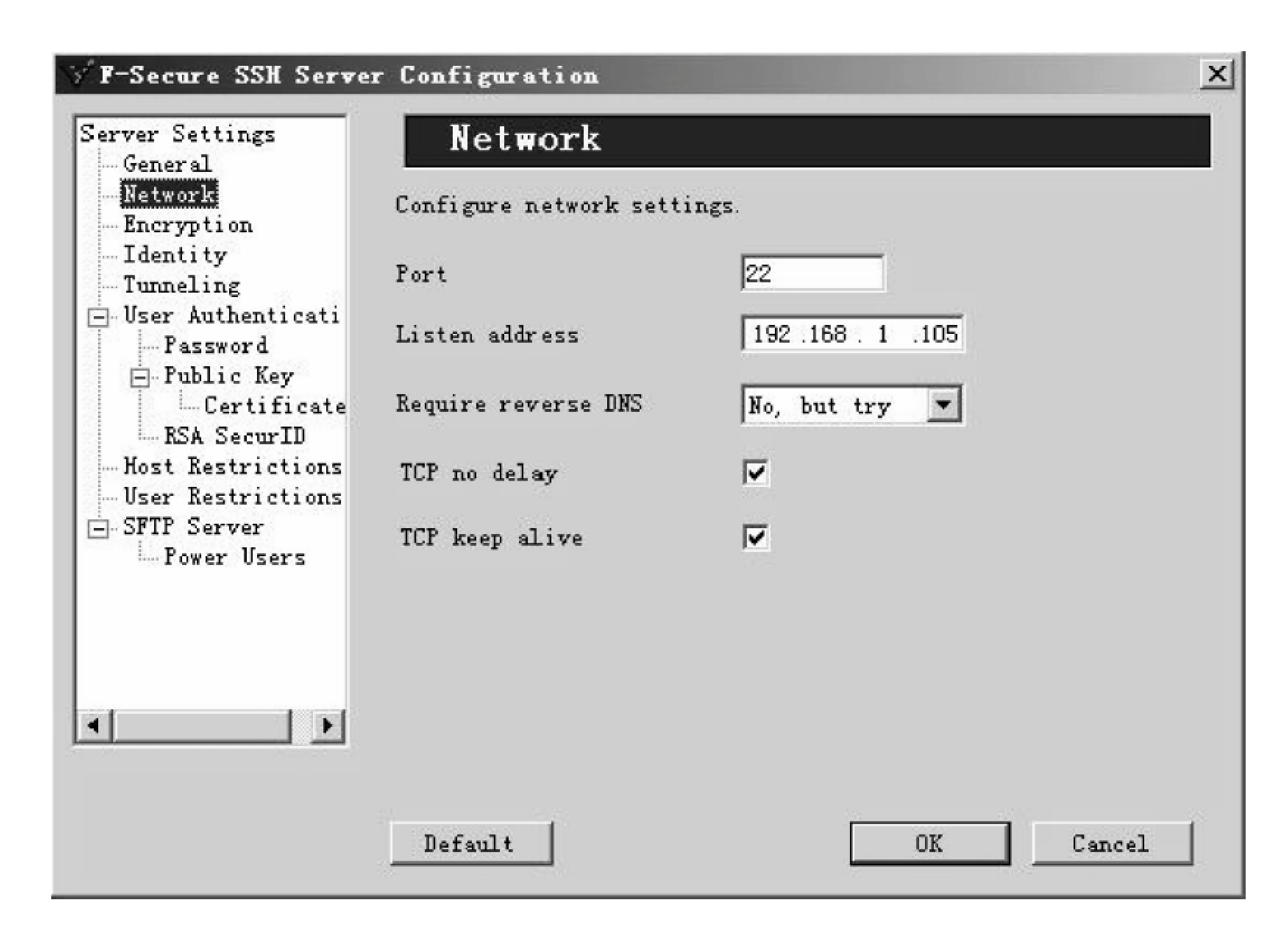


图 11.7　配置服务器的 IP 地址

“SSH＝c:\SSHDirectory”，然后单击 Apply 按钮，最后单击“确定”按钮，如图 11.8 所示。

在 Windows XP 中，依次单击“开始”→“所有程序”→SSH Secure Shell、Secure Shell Client，打开 SSH Secure File Transfer 窗口。在该窗口中的工具栏中选择 Connection 按钮，打开 Connect to a Remote Host 对话框，如图 11.9 所示。

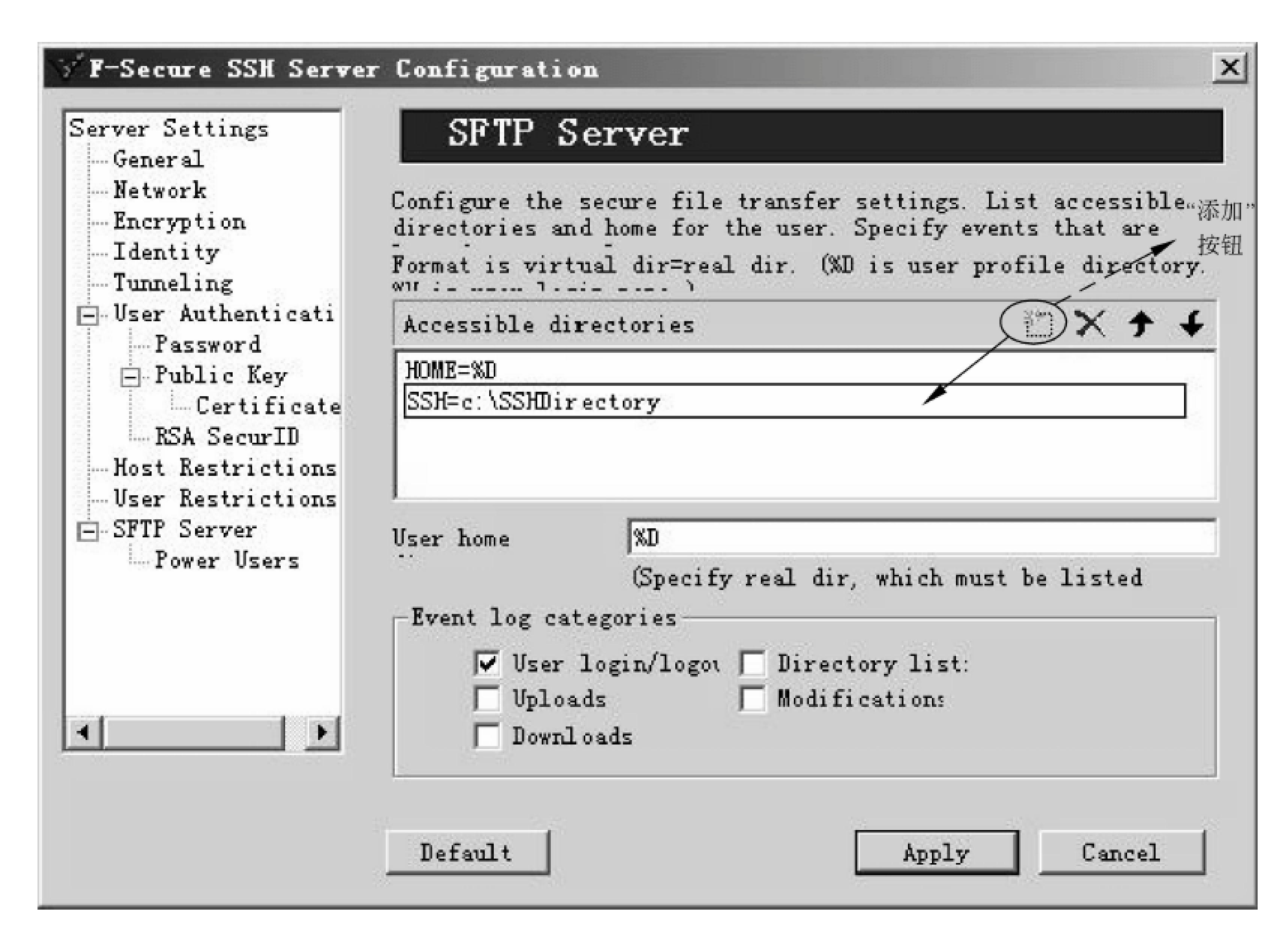


图 11.8　添加自定义目录

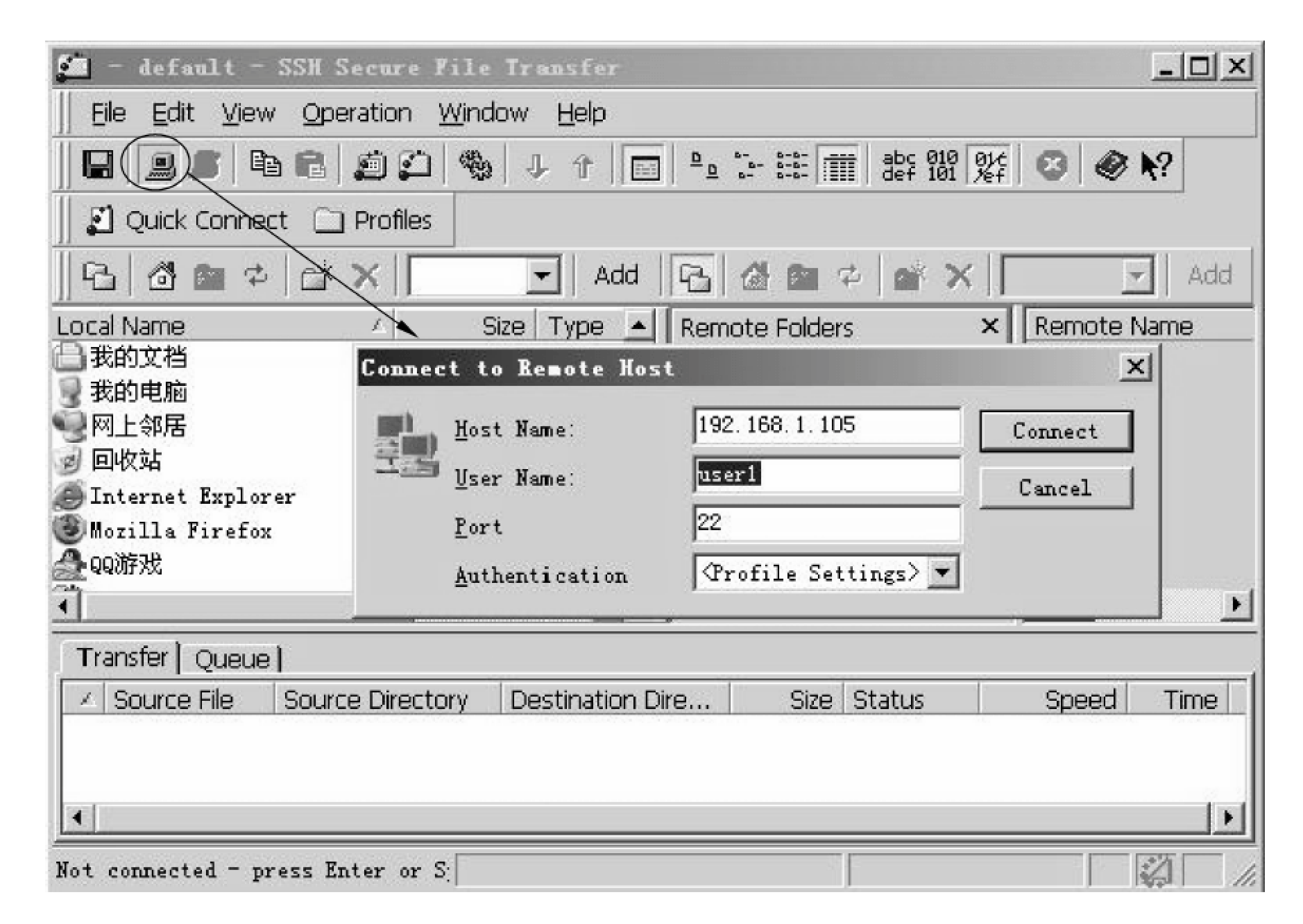


图 11.9　连接远程服务器

在 Connect to a Remote Host 对话框中输入远程服务器的 IP 地址，以及在服务器上创建的用户名 user1。单击“Connect”按钮。在弹出的对话框中输入该用户名对应的口令。如图 11.10 所示。

若输入的口令正确，则客户端就会呈现远程服务器中目录的内容，如图 11.11 所示，其

中 Home 目录是 user1 的默认目录，SSH 目录是用户自定义的目录。然后通过拖动文件，就可实现文件在客户端与服务器之间的安全传递。

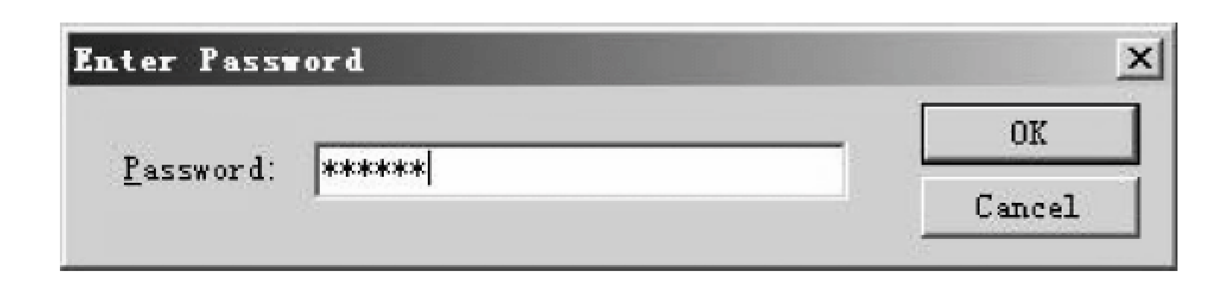


图 11.10　输入 user1 的登录口令

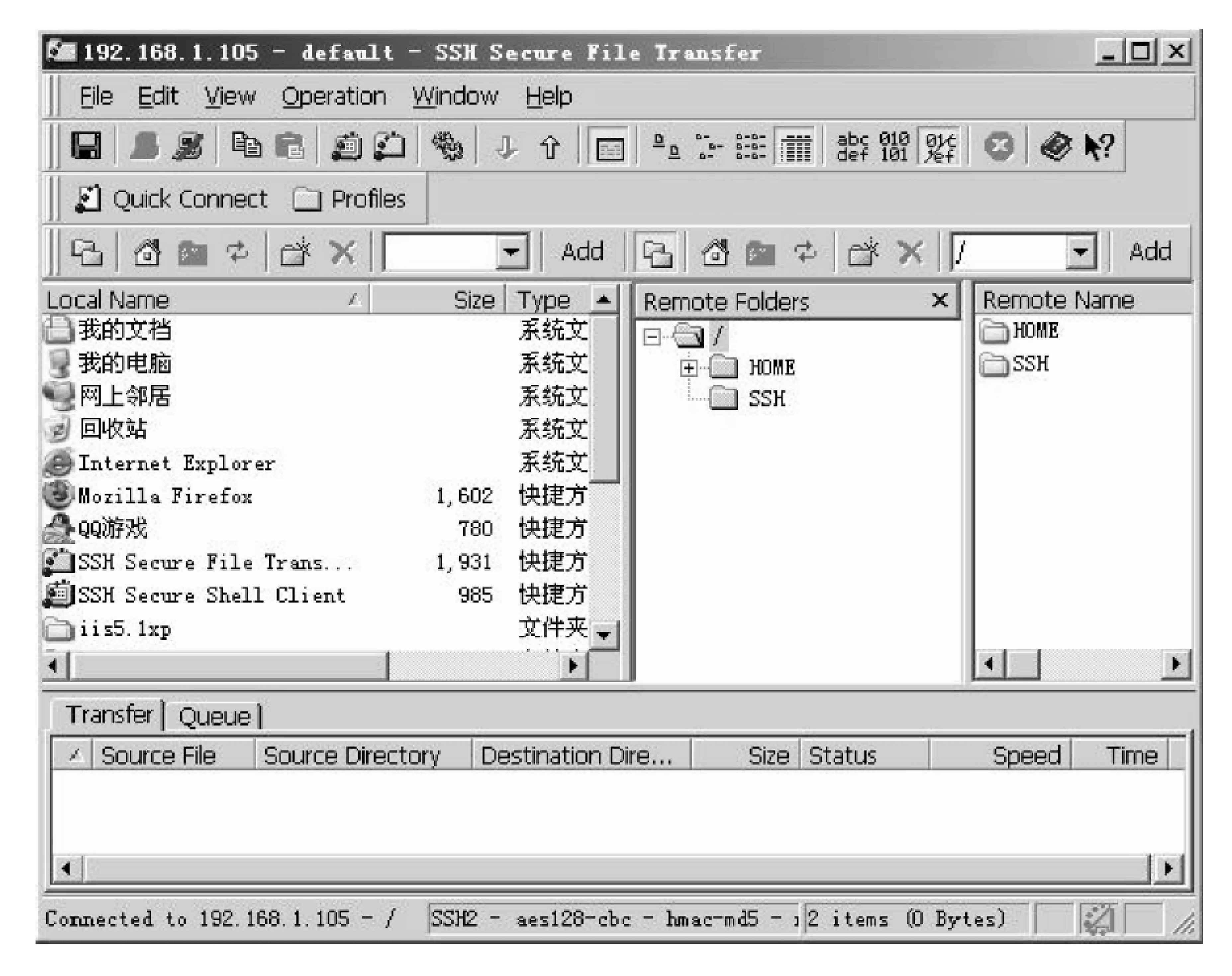


图 11.11　SSH Client 的主界面

注：在 SSH 客户端中输入的口令在网络上是以密文形式传递的，这一点可以通过 Sniffer 工具来验证。

11.5.2　更新服务器的主密钥

为了支持服务器的公钥认证方式，服务器在安装后会产生一对非对称密钥对(包含公钥和私钥)，其中公钥在客户机第一次连接服务器时，由服务器传递给客户机进行保存。当服务器端运行一段时间后，为了保证 F-Secure SSH 的安全，可以为服务器端更新非对称密钥对，步骤如下。

首先在 F-Secure SSH Server 的主配置窗口的左边选中 Identify，然后在右边的窗口中单击 Generate 按钮，则会运行 SSH_keygen2.exe，产生新的公私密钥对。如图 11.12 和图 11.13 所示。

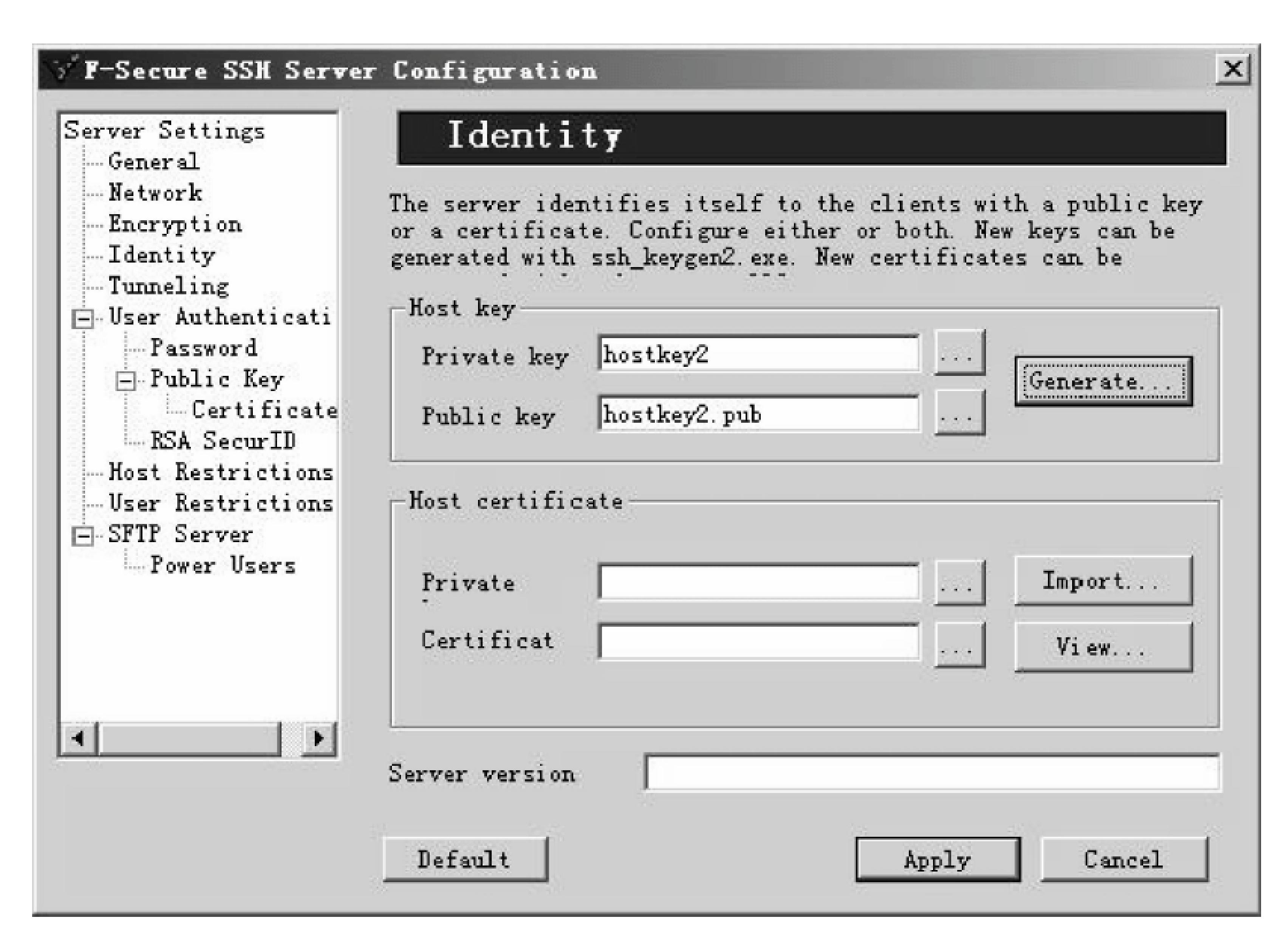


图 11.12　更新密钥对的窗口

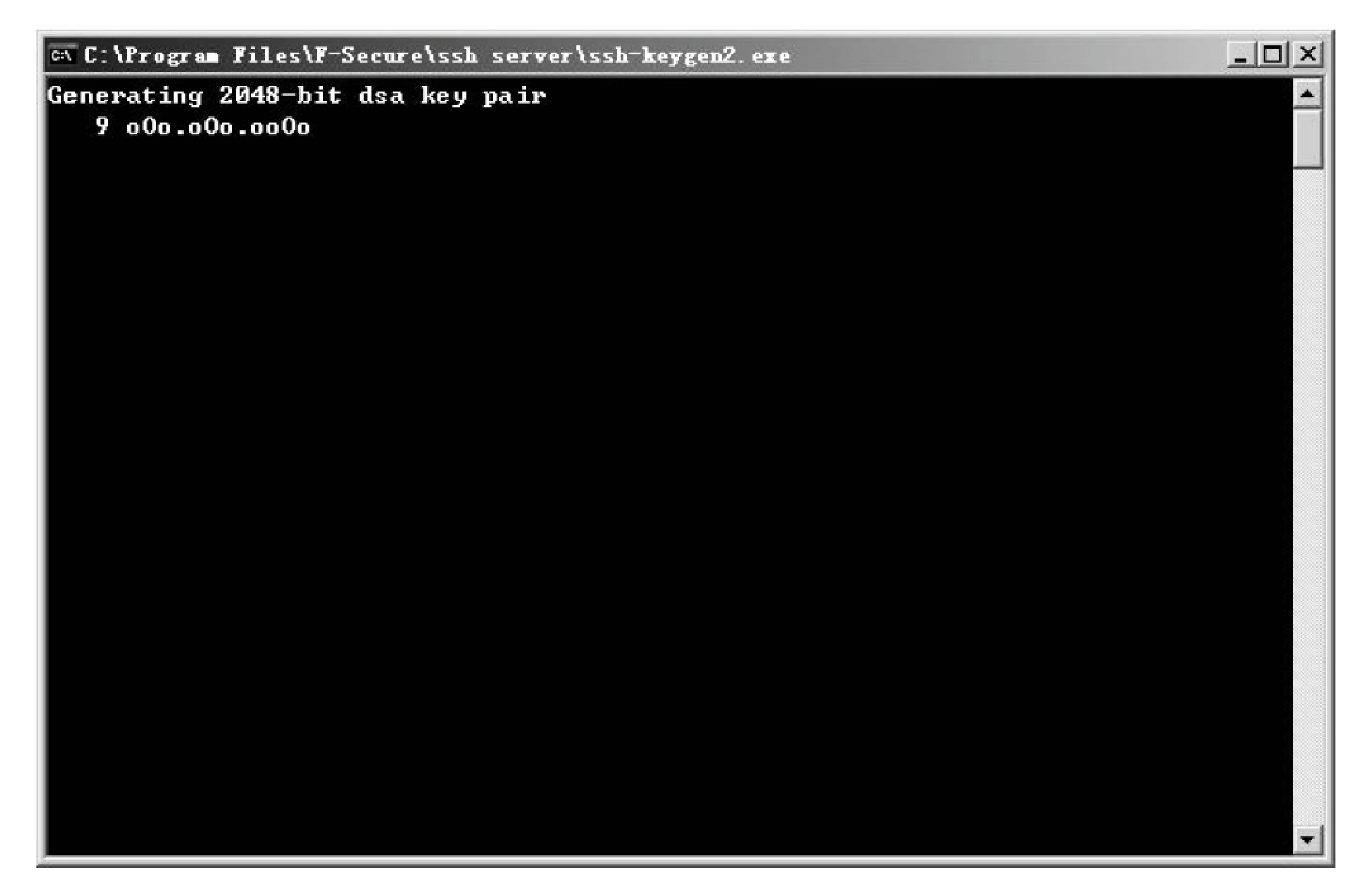


图 11.13　SSH-keygen2 运行的界面

当服务器的密钥对更新完毕后，若客户端连接到服务器，则会弹出一个告警窗口，提示用户服务器的主密钥已经更新，如图 11.14 所示。

当用户在图 11.14 中单击 Yes 后，会弹出另一个窗口，提示用户接收新的服务器公钥。同样需要单击 Yes，如图 11.15 所示。

HOST IDENTIFICATION HAS CHANGED

WARNING: HOST IDENTIFICATION HAS CHANGED!
1. Either the administrator of the remote host computer has changed the host identification, or
2. The SSH protocol has been upgraded from SSH1 to SSH2, or
3. SOMEONE COULD BE EAVESDROPPING ON YOU RIGHT NOW (man-in-the-middle attack)!

It is NOT RECOMMENDED to connect to the remote host computer until you have contacted the system administrator and found out why the host identification has changed.

The fingerprint of the host public key is:
"xoteb-gykos-zetir-vivuz-mimoh-zinis-kacev-luhyh-kysyn-vozec-byxyx"

Do you want to continue with the connection?

Yes No Help

图 11.14 提示服务器密钥对已更新



图 11.15 提示用户接收新的服务器公钥

11.6 实验思考

(1) 结合实验 9 中的 Sniffer 实验，来验证使用 F-Secure SSH 进行远程登录时，是否把用户的口令加密了。

(2) 如何利用 F-Secure SSH 工具进行基于密钥的认证，即用户和服务器通过公私密钥对进行相互的认证(并非基于 PKI 架构的认证)。

实验12 IIS 安全配置实验

12.1 实验目的与要求

掌握 IIS 的基本安全配置方法。

12.2 实验环境

装有 Windows 2003 Server 的 PC 一台。

12.3 预备知识

IIS(Internet Information Services,互联网信息服务)是一款由微软公司提供的、运行于 Windows 平台上的一种互联网基本服务,其内置在 Windows 2000、Windows XP Professional 以及 Windows Server 2003 中,而 Windows XP Home 版不支持 IIS。目前常见的 IIS 版本有支持 Windows 2000 的 IIS 5.0、支持 Windows XP Professional 和 Windows XP Media Center Edition 的 IIS 5.1、支持 Windows Server 2003 与 64 位 Windows XP Professional x64 的 IIS 6.0、支持 EditionWindows Server 2008 和 Windows Vista 的 IIS 7.0 以及支持 Windows Server 2008 R2 and Windows 7 的 IIS 7.5。

IIS 作为当前最为流行的 Web 服务器之一,能够提供强大的 Internet 和 Intranet 服务。它不仅能够提供超文本传输协议,以便于用户自行架设网站,还能够通过配置提供文件传输协议(FTP)、网络新闻传输协议(NNTP)以及简单邮件传输协议(SMTP)服务等。

IIS 具有强大的网络功能,但是其安全问题也不容忽视。早期的 IIS 版本均存在许多的安全脆弱性,比如容易遭受著名的红色代码攻击。而在后期的版本中,如 IIS 6.0 以及 IIS 7.0,其安全性有所加强。例如,在 IIS 6.0 中,微软对先前的预安装 ISAPI 行为进行了修正,从而弥补了在 4.0 版和 5.0 版中出现的若干漏洞。此外,在 IIS 6.0 还增加了 Web 服务扩展(Web Service Entensions)的功能,这使得 IIS 在取得系统管理员的明确授权之前无法发布任何程序。

下面,我们以 IIS 6.0 为例,介绍一下如何对 IIS 进行安全配置,以增

强其安全性。

12.4 实验内容

本章的实验内容主要包括以下两部分：

(1) 演示如何在 Windows 2003 Server 上安装 IIS 6.0，并且为了确保 IIS 运行的安全性，演示如何对 Windows 系统进行两方面的加固，即一般性安全保护和 TCP/IP 的安全配置。

(2) 演示如何对 IIS 6.0 自身进行安全配置，以减少 IIS 自身存在的安全隐患。

12.5 实验步骤

12.5.1 IIS 6.0 的安装

单击“开始”→“控制面板”→“添加/删除程序”→“添加/删除 Windows 组件”命令，选中“应用程序服务器”前的复选框，如图 12.1 所示。然后单击图 12.1 右下方的“详细信息”按钮，可以安装 IIS 的各个组件。在这些组件中，默认选项有 ASP.NET、“Internet 信息服务(IIS)”以及“启用网络 COM+访问”，而“启用网络 DTC 访问”、“消息队列”以及“应用程序服务器控制台”为可选项。单击“下一步”按钮，按照提示便可完成 IIS 6.0 的安装。

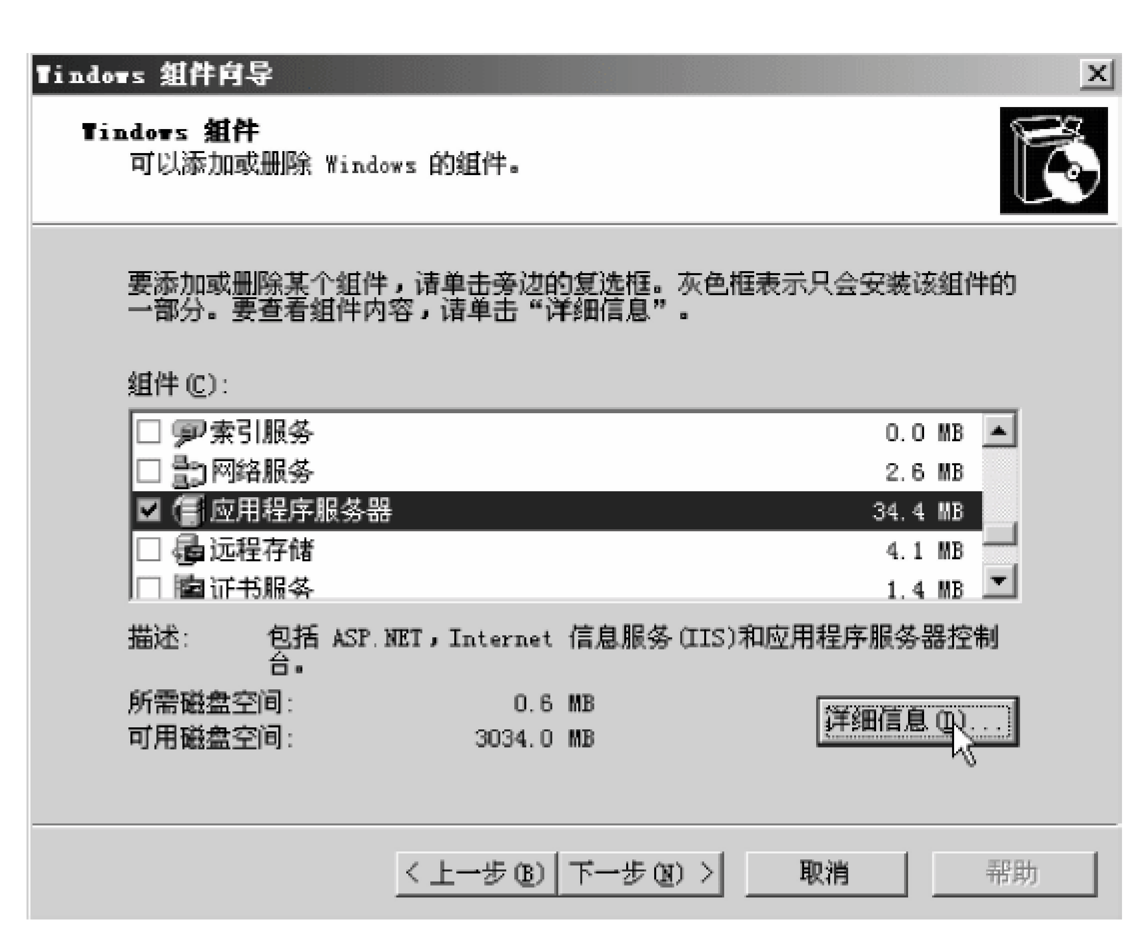


图 12.1 安装 IIS

安装完 IIS 后，首先需要对系统进行安全加固操作，以确保 IIS 所处的系统环境的安全性。这项工作分为以下两个方面：

1. 一般性安全保护

(1) 选择“开始”→“所有程序”→ Windows Update 来实现系统补丁的安装。

(2) 安装杀毒软件，并更新病毒库。

(3) 安装其他安全软件，进行系统漏洞的扫描，并修补所有的安全漏洞。

(4) 进行系统的备份，如采用 Ghost 软件备份系统。

2. TCP/IP 安全配置

(1) 右键单击“网上邻居”,在弹出的对话框中选择“属性”,从而打开“网络连接”对话框。

(2) 在“网络连接”对话框中右键单击“本地连接”,从而打开“本地连接 属性”对话框。在该对话框中删除不必要的网络协议和服务,并保留 Internet 协议(TCP/IP)。同时为了控制带宽流量,需要安装 QoS 数据包计划服务:首先将 Windows 2003 安装盘装入光驱,然后在“本地连接 属性”对话框中单击“安装”按钮,在弹出的“选择网络组件类型”对话框中双击“服务”选项,则会弹出“选择网络服务”对话框,在该对话框的左边“厂商”一栏选择 Microsoft,在右边的“网络服务”一栏选择“QoS 数据包计划程序”,单击“确定”按钮即可,如图 12.2 所示。

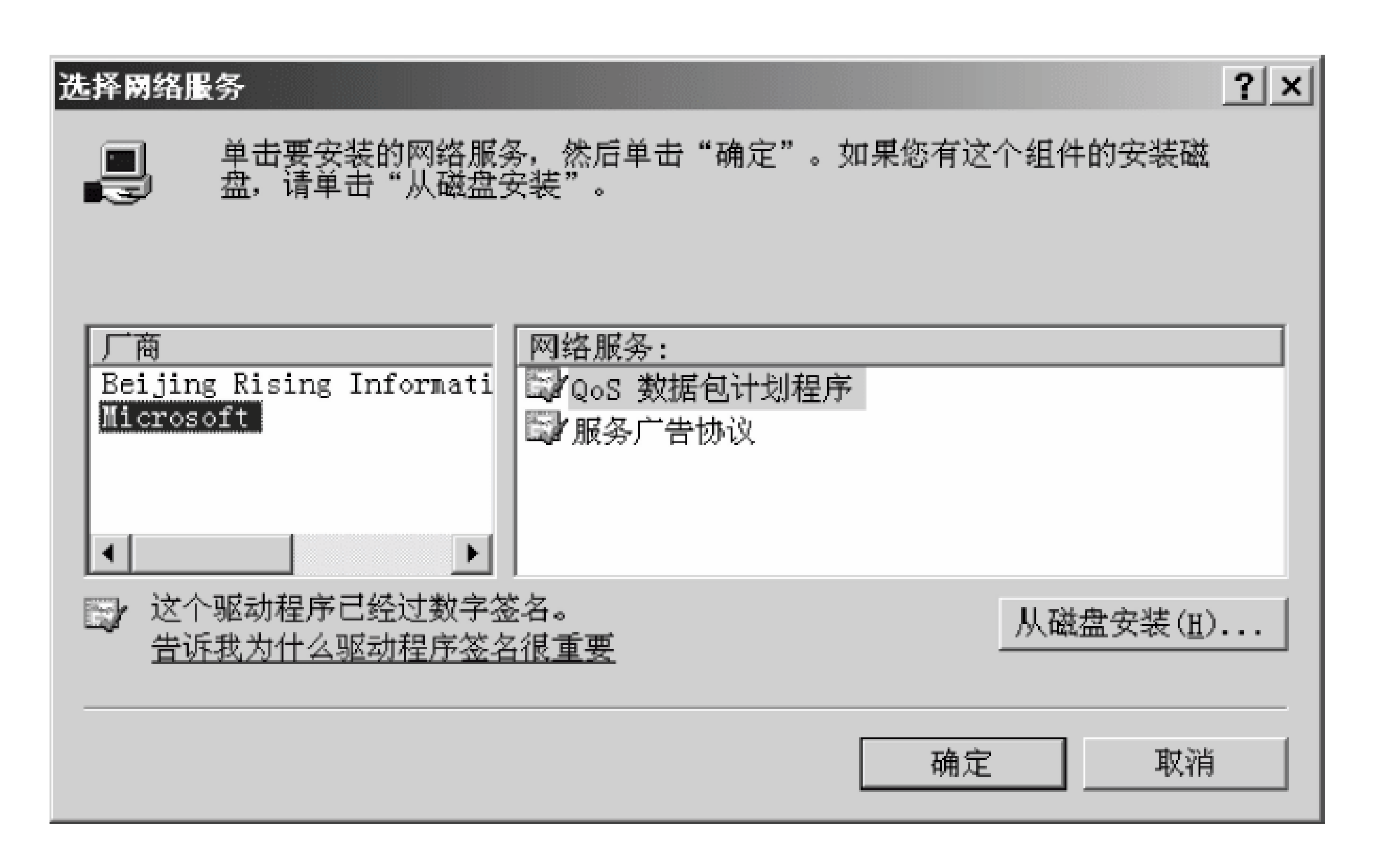


图 12.2 安装 QoS 数据包计划

(3) 在“本地连接 属性”对话框中选择 Internet 协议(TCP/IP),然后单击右下方的“属性”按钮,打开“Internet 协议(TCP/IP) 属性”对话框。单击该对话框右下方的“高级”按钮,打开“高级 TCP/IP 设置”对话框。首先选择该对话框中的 WINS 属性页,在下方的 NetBIOS 设置中选择“禁用 TCP/IP 上的 NetBIOS(S)”,如图 12.3 所示;然后选择该对话框的“选项”属性页,在该属性页中选择“TCP/IP 筛选”,并单击右下方的“属性”,打开“TCP/IP 筛选”对话框,在该对话框中首先在“启用 TCP/IP 筛选(所有适配器)”复选框前打钩,并进行许可端口的设置,如图 12.4 所示。

12.5.2 IIS 相关安全配置

1. 站点的存放及日志的开启

首先关闭并删除默认站点。然后在建立自己的站点时,为了防止系统崩溃不会对站点文件造成影响,可将站点文件放在一个与系统目录不同的分区中,如 D 盘下。为了审计站点是否遭受攻击,对站点进行日志记录是十分必要的。在 IIS 中,可以选择“W3C 扩展日志文件格式”对站点进行日志的记录,具体操作如下。

打开“Internet 信息服务(IIS)管理器”对话框,在左边一栏右键单击自己的网站,在弹出

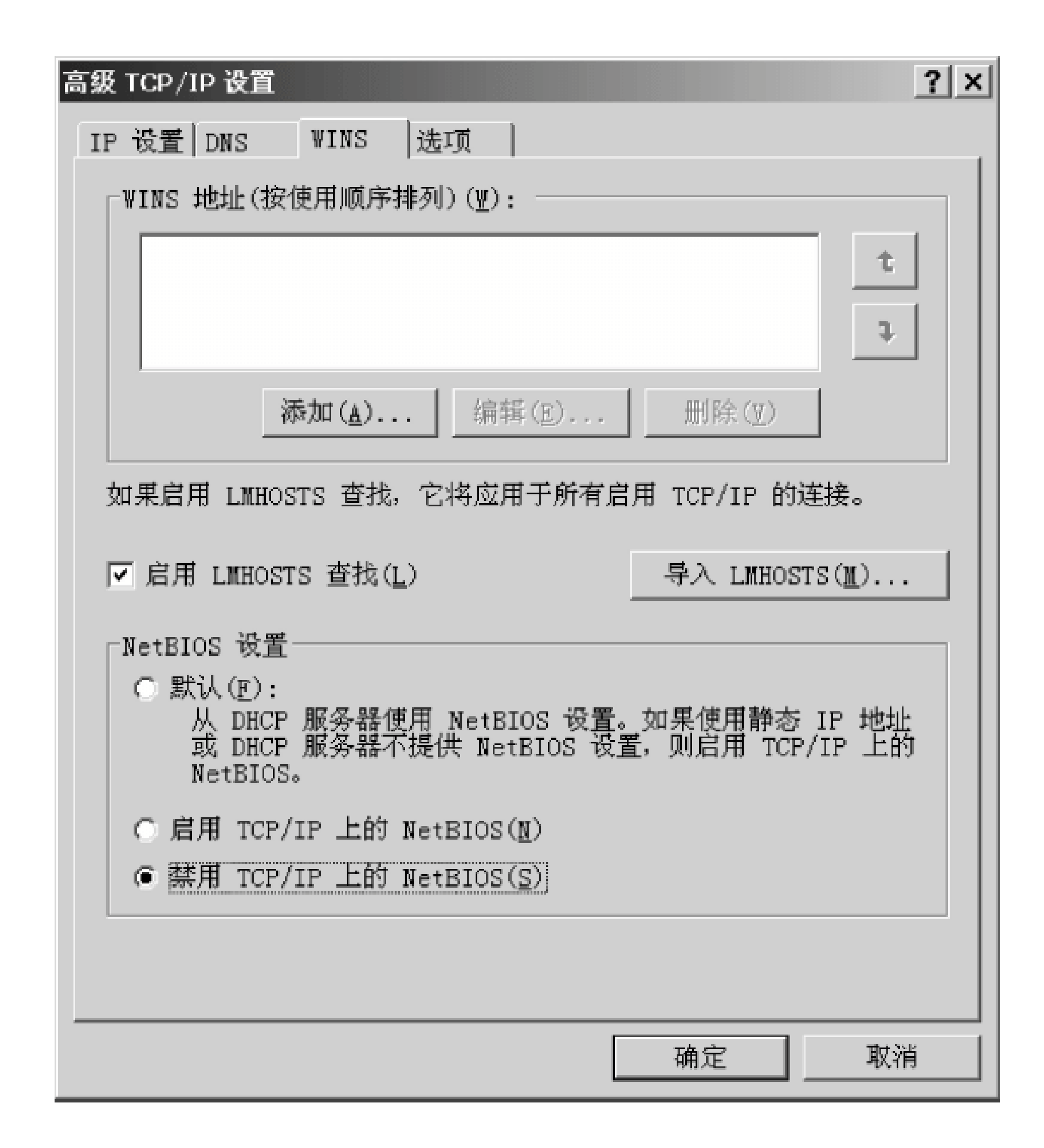


图 12.3　禁用 TCP/IP 上的 NetBIOS 选项

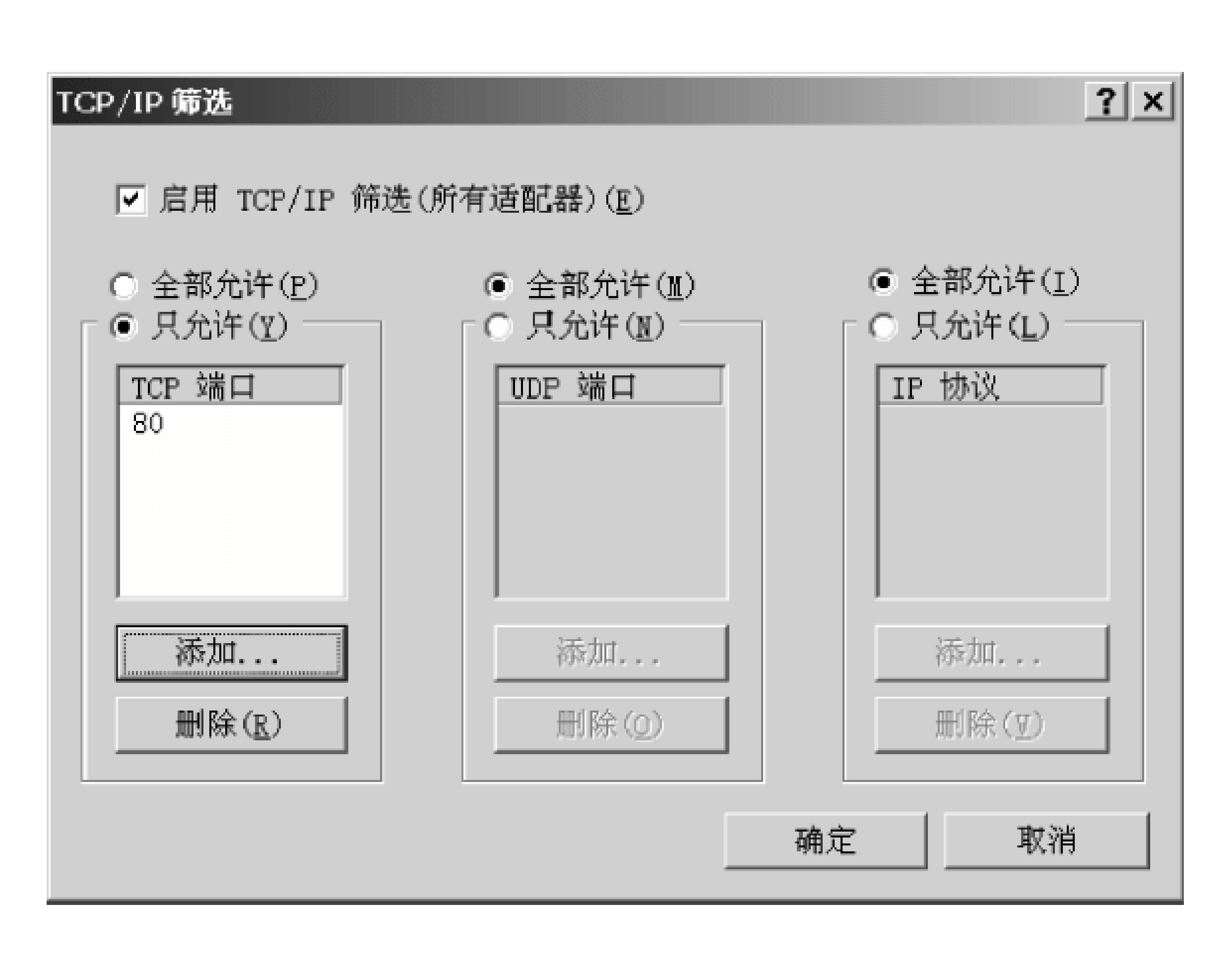


图 12.4　端口筛选

的网站属性对话框中选择“网站”选项卡。在该选项卡中，选中“启用日志记录”，并单击右下方的“属性”按钮，弹出“日志记录属性”对话框。在该对话框中选择“高级”选项卡，并选中下面的扩展属性：客户 IP 地址、用户名、方法、URI 资源、http 状态、Win32 状态、用户代理、服务器 IP 地址、服务器端口，如图 12.5 所示。

为了确保日志文件的安全性，可以在一个与站点文件不同的分区，如 E 盘下建立一个审计目录 Log，并通过 IIS 设置，使得建立站点时的日志文件均置于此目录中，具体操作如下。

在“日志记录属性”对话框中，选择“常规”选项卡，并在下面的“日志文件目录”一栏中将日志存放目录设置为 E:\Log，如图 12.6 所示。



图 12.5　日志记录设置



图 12.6　日志目录

同时,为了确保该目录的安全性,应该将该目录的访问权限设置为仅:Administrators(完全控制)和 System(完全控制)。

2. 删除不必要的 IIS 映射和扩展

为了使用的方便,IIS 被预置为支持.asp 和.shtm 文件的扩展名。每当 IIS 服务器接收到这些类型的文件请求时,则自动由 DLL 进行处理。如果不使用其中的一些扩展和功能,为了安全考虑,则应该删除这些默认的文件映射,具体步骤如下。

打开“网站属性”对话框，并选择“主目录”选项卡。在该选项卡的右下方选择“配置”按钮，打开“应用程序配置”对话框，选择“映射”选项卡，在“应用程序扩展”一栏删除扩展名为.htw、.htr、.idc、.ida、.idq 和.printer 的选项，如图 12.7 所示。



图 12.7 删除默认映射

3. 禁用父路径

“父路径”选项允许在对诸如 MapPath 函数调用中使用“..”。在默认情况下，该选项处于启动状态，为了安全考虑应将其禁用，禁用操作步骤如下。

打开“应用程序配置”对话框，选择“选项”选项卡，然后取消“启用父路径”前面复选框中的钩，如图 12.8 所示。



图 12.8 禁用父路径

4. 设置虚拟目录的访问控制权限

为了减少被攻击的可能性，应该对网站中不同类型的文件设置不同的访问控制权限，具体如下。

- 扩展名为.exe、.dll、.cmd 和.pl 等的文件应该由 Administrators 和 System 组完全控制，而 Everyone 组无权访问。
- 扩展名为.asp 的文件由 Administrators 和 System 组完全控制，而 Everyone 组无权访问。
- 扩展名为.inc、.shtm 和.shtml 等的文件由 Administrators 和 System 组完全控制，而 Everyone 组无权访问。
- 扩展名为.txt、.gif、.jpg 和.html 等的文件由 Administrators 和 System 组完全控制，而 Everyone 组具有只读权限。

在创建 Web 站点时，为了控制的灵活起见，没有必要为每个文件设置访问权限，应该为每个文件类型创建一个新的目录，然后在每个目录上设置访问权限，允许访问控制权限传给每个文件。为了做到这一点，需要进行如下操作。

① 右键单击网站文件所在的目录，在弹出的快捷菜单中选择“属性”选项，打开目录的“属性”对话框，在该对话框的“组或用户名称”一栏选中所需的组，并在下方设置相应的权限。

② 单击“属性”对话框右下方的“高级”按钮，选择“权限”选项卡，在“权限项目”一栏中选中所需的组或用户，并单击下方的“编辑”按钮，打开“权限目录”对话框，在该对话框中的“应用到”一栏选择“该文件夹、子文件夹及文件”，并单击“确定”按钮，如图 12.9 所示。

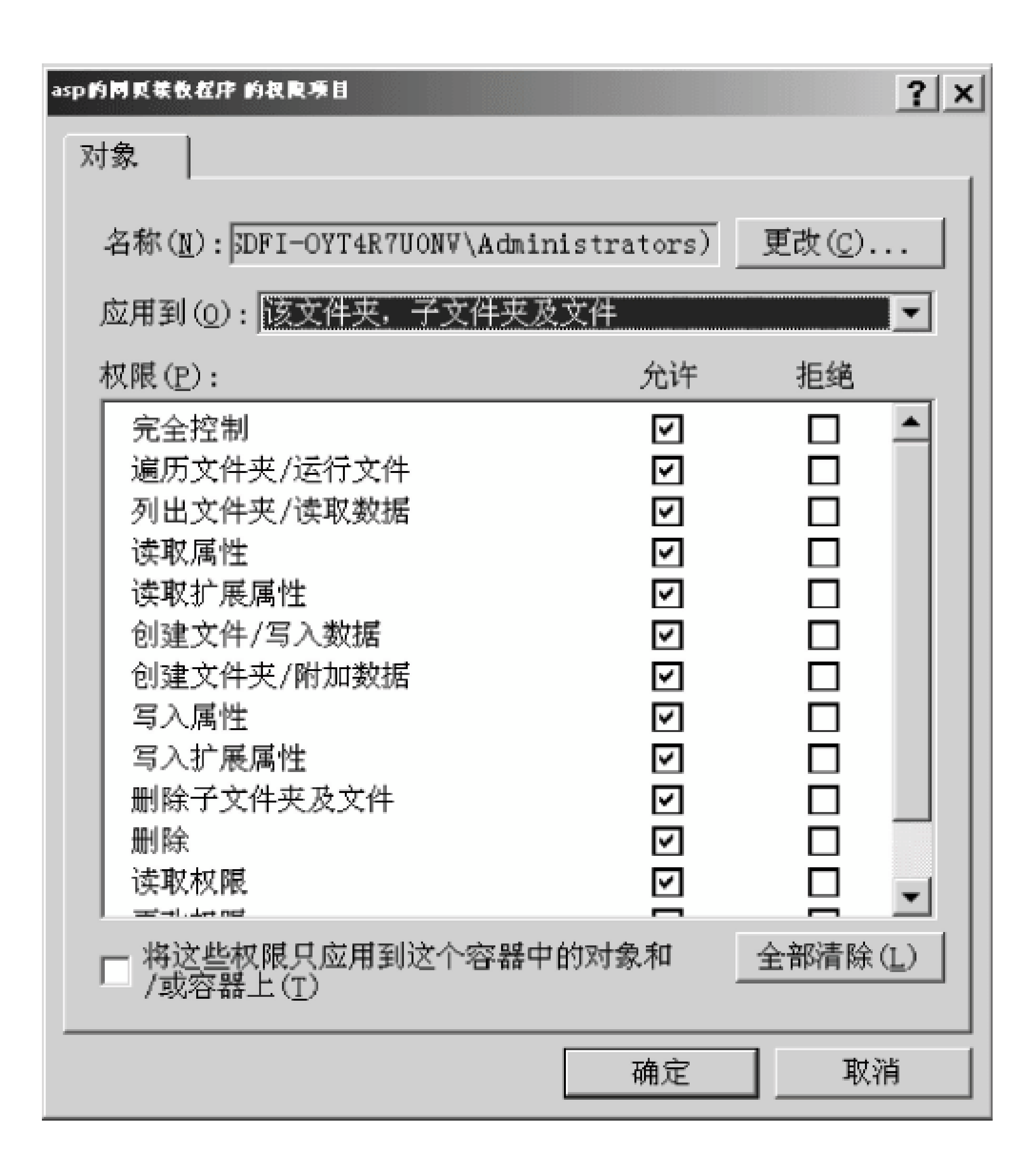


图 12.9 设置虚拟目录的访问权限

通过上述对安装 IIS 的 Windows 系统和 IIS 自身进行的安全配置，可以打造出一个较为安全的 IIS 运行环境，能够防止由于配置不当造成的安全隐患。但是，如果想要打造一个

更安全的 Web 网站,那么还需要综合 Web 网站的安全设计、防火墙以及入侵检测和防御系统等技术来共同实现。

12.6 实验思考

(1) 为什么在安装了 IIS 6.0 后,需要禁用 NETBIOS?

(2) 若 IIS 6.0 中挂载了 FTP 服务,那么还需要对 IIS 6.0 进行哪些安全配置?



Windows 2000 系统中 SSL 的实现

13.1 实验目的与要求

掌握利用 Windows 2000 Server 的 IIS 服务与证书颁发机构建立 SSL 服务，以实现涉密 Web 业务的安全传输。

13.2 实验环境

运行 Windows 2000 Server 操作系统的服务器一台，安装 IIS 5.1 组件与证书颁发机构组件；运行 Windows 2000 Perfessional 操作系统的客户机一台。

13.3 预备知识

13.3.1 SSL/TLS 协议

SSL(Security Socket Layer，安全套接层)协议为 Netscape 公司于 1994 年提出的基于 Web 应用的安全协议，目前最高版本为 3.0。IETF (Internet Engineering Task Force，Internet 工程任务组)在 SSL 3.0 协议规范之上制订了一种新的安全协议 TLS(Transport Layer Security，传输层安全协议)，是 SSL 3.0 的后续版本。TLS 与 SSL 的主要区别在于支持的加密算法不同，因此两者不能互操作。目前 IE 6.0 以上浏览器版本支持 SSL 2.0、SSL 3.0 与 TLS 1.0 。

SSL/TLS 提供的安全服务包括：

- 认证服务器的真实性。
- 认证客户机真实性。
- 确保涉密数据的保密性。
- 给数据添加鉴别码，确保数据的完整性。

SSL/TLS 协议的工作流程如下：

(1) 客户端浏览器将其支持的 SSL 版本号、加密设置参数、与 Session 有关的数据以及其他一些必要信息发送到服务器。

(2) 服务器在收到的信息中选择其支持的 SSL 版本号、加密设置参数、与 Session 有关的数据以及其他一些必要信息发送给客户端浏览器，同时发给浏览器的还有服务器的证书。如果服务器需要验证客户身份，则要求浏览器提供客户证书。

(3) 客户端检查服务器证书，如果检查失败，则提示不能建立 SSL 连接；如果成功，则继续。

(4) 客户端浏览器为本次会话生成 Pre-master secret，并将其用服务器公钥加密后发送给服务器。

(5) 如果服务器要求鉴别客户身份，客户端还要对另外一些数据签名后并将其与客户端证书一起发送给服务器。

(6) 如果服务器要求鉴别客户身份，则检查签署客户证书的 CA 是否可信。如果不在信任列表中，结束本次会话。如果检查通过，服务器用自己的私钥解密收到的 Pre-master Secret，并用它通过某些算法生成本次会话的 Master secret。

(7) 客户端与服务器均使用此 Master secret 生成本次会话的会话密钥(对称密钥)。在双方 SSL 握手结束后传递任何消息均使用此会话密钥。这样做的主要原因是对称加密比非对称加密的运算速度快。

(8) 客户端通知服务器此后发送的消息都使用这个会话密钥进行加密。并通知服务器客户端已经完成本次 SSL 握手。

(9) 服务器通知客户端此后发送的消息都使用这个会话密钥进行加密，并通知客户端服务器已经完成本次 SSL 握手。

(10) 本次握手过程结束，会话已经建立。双方使用同一个会话密钥分别对发送以及接收的信息进行加、解密。

13.3.2 HTTPS 介绍

HTTPS(Secure Hypertext Transfer Protocol，安全超文本传输协议)是由 Netscape 公司基于 HTTP 技术开发的并内置于浏览器中的安全协议，用于对网络上传输的数据进行压缩/解压缩和加密/解密操作。HTTPS 的安全基础是 SSL，即在 HTTP 协议中加入 SSL 协议来实现安全的 Web 传输。HTTPS 使用端口 443，而不是像 HTTP 那样使用端口 80 来和 TCP/IP 进行通信。

13.4 实验内容

本章的实验内容主要包括以下几部分：

(1) 演示如何在证书服务器中安装证书服务，以便提供证书的制作服务。

(2) 演示如何配置 IIS 服务器，以便产生一个 IIS 服务器证书请求文件。

(3) 演示如何利用 IIS 服务器证书请求文件向证书服务器请求 IIS 服务器证书。

(4) 演示证书服务器如何利用证书请求文件颁发 IIS 服务器证书。

(5) 演示如何在 IIS 中安装申请得到 IIS 服务器证书。

(6) 演示如何在 IIS 中结合已安装的证书配置 SSL 协议。

(7) 演示 SSL 的测试方法。

13.5 实验步骤

13.5.1 证书服务安装

在 Windows 2000 Server 服务器端的控制面板里面选择“添加删除程序”。选择“证书服务”。单击“确定”按钮，将出现如图 13.1 所示提示。

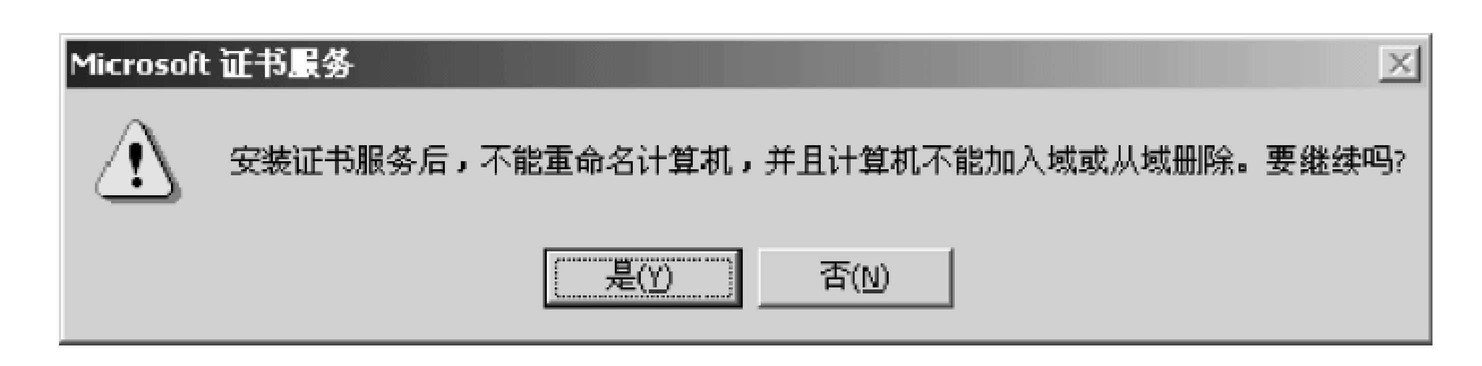


图 13.1 证书服务安装提示

在图 13.1 中单击“是(Y)”按钮，出现如图 13.2 所示的对话框。

Windows 组件向导
Windows 组件
可以添加或删除 Windows 2000 的组件。
要添加或删除某个组件，请单击旁边的复选框。灰色框表示只会安装该组件的一部分。要查看组件内容，请单击“详细信息”。
组件(C):
远程存储 3.5 MB
证书服务 1.4 MB
终端服务 14.3 MB
终端服务授权 0.9 MB
描述: 将计算机配置成为终端服务许可证服务器以便提供客户端许可证。
所需磁盘空间: 11.4 MB
可用磁盘空间: 5198.6 MB
详细信息(D)...
< 上一步(B) 下一步(N) > 取消

图 13.2 选择“证书服务”

在图 13.2 中选中“证书服务”复选框，然后单击“下一步”按钮，系统进行证书服务安装，并显示如图 13.3 所示的对话框。

在图 13.3 中填写必要的信息，然后单击“下一步”按钮，按提示继续操作，直到出现如图 13.4 所示的提示，单击“确定”按钮即可。

13.5.2 配置 IIS 服务器

选择“开始”→“程序”→“管理工具”→“Internet 服务器管理”命令，打开“Internet 信息服务”对话框，单击“默认站点”→“属性”，如图 13.5 所示。



图 13.3 填写 CA 信息

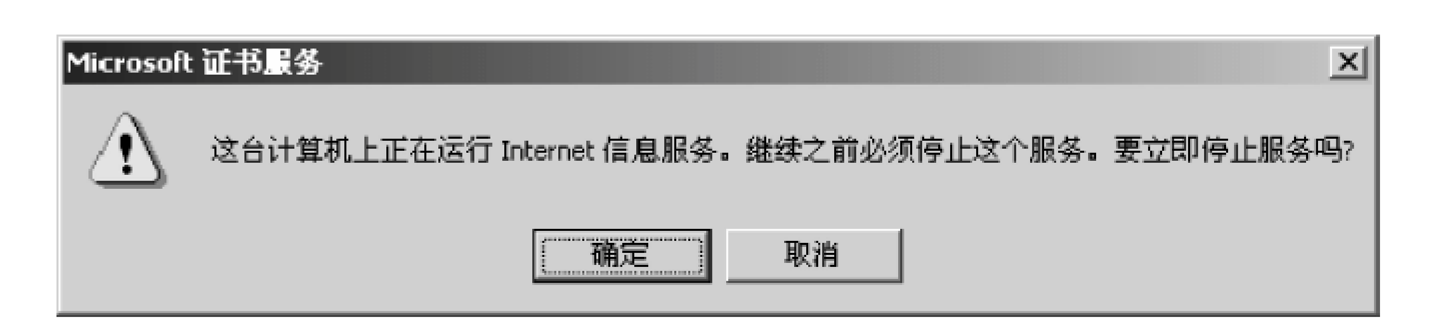


图 13.4 安装证书服务提示

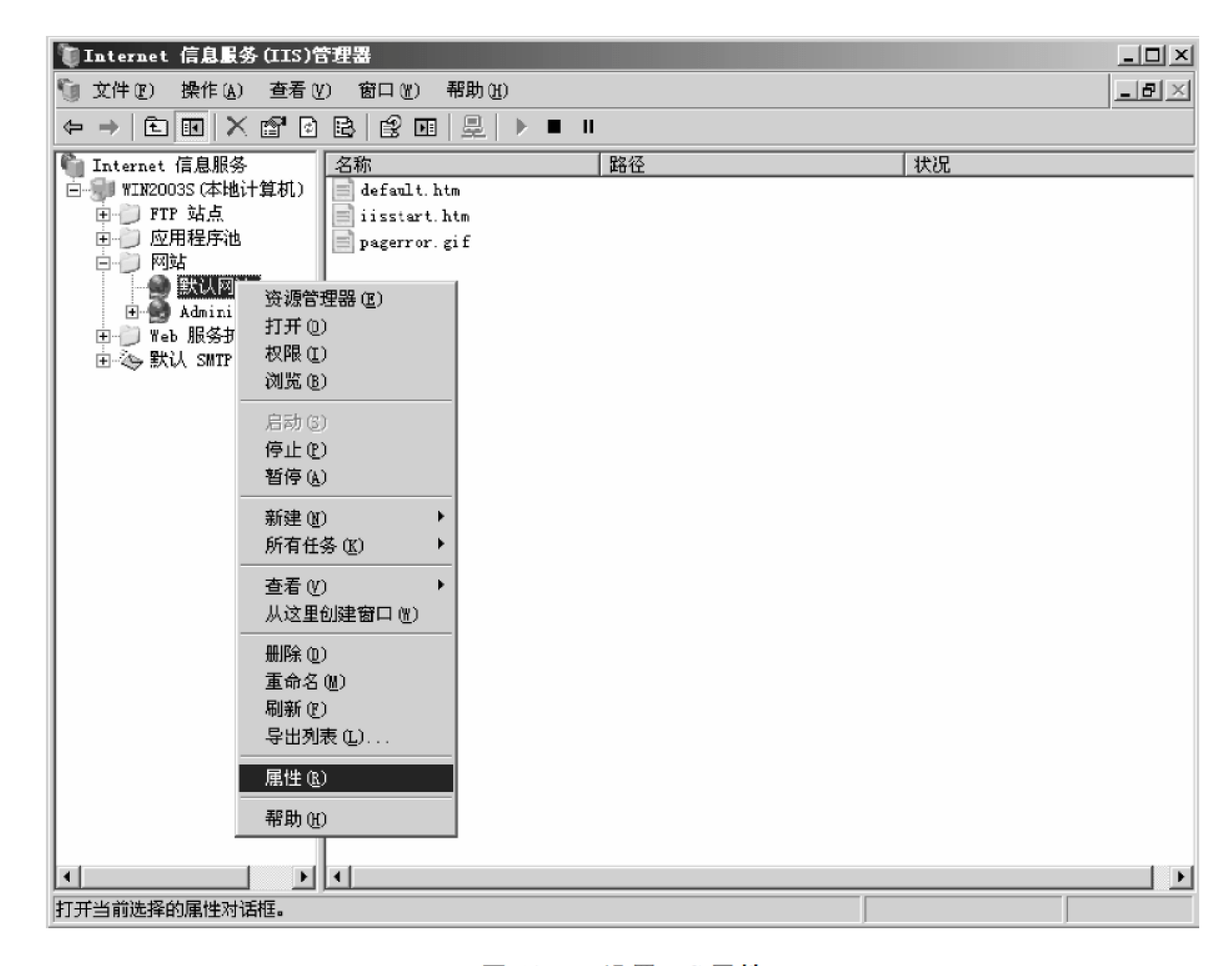


图 13.5 设置 IIS 属性

在弹出的如图 13.6 所示的“默认 Web 站点属性”对话框中，选择“目录安全性”选项卡。

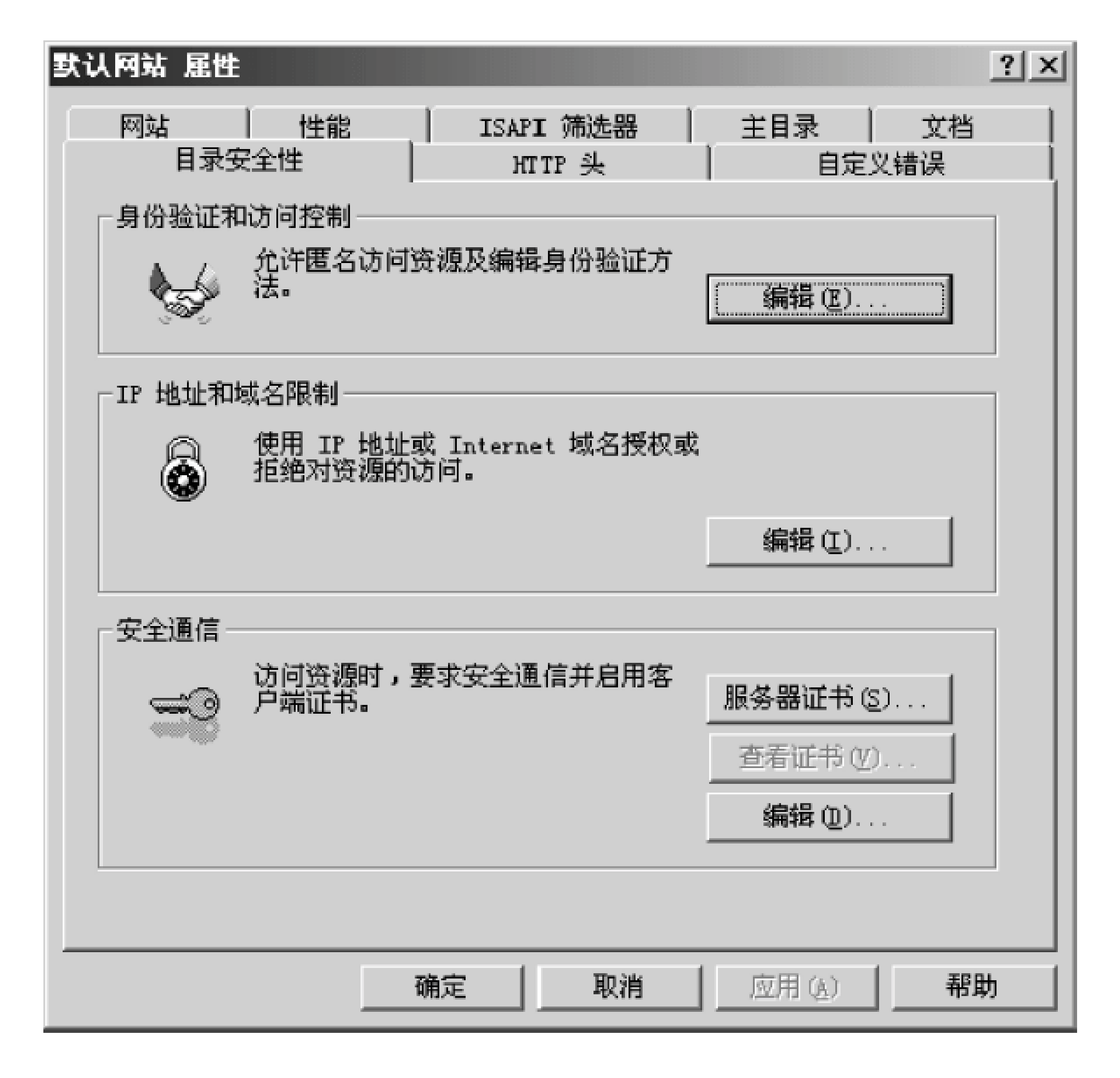


图 13.6 “目录安全性”选项卡

开始配置服务器证书。单击“服务器证书”→“下一步”→“创建一个新证书”，出现如图 13.7 所示的对话框，考虑到信息安全性，在“位长”一栏选择“1024”。

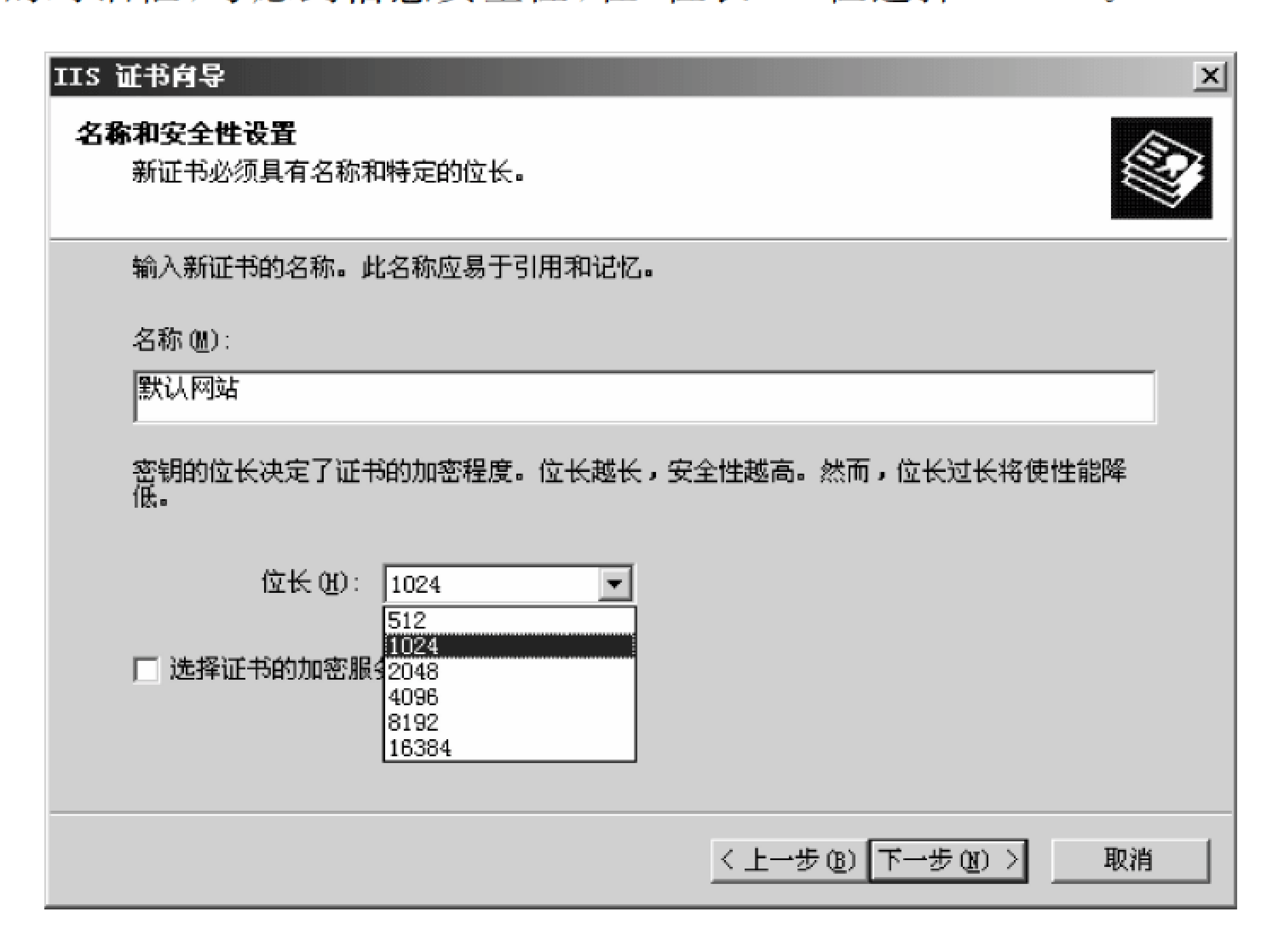


图 13.7 选择密钥长度

按照提示单击“下一步”按钮，直到出现如图 13.8 所示的对话框，务必记住文件路径，默认是 c:\certreq.txt。

certreq.txt 文本文件中的内容即是向证书服务器申请 IIS 服务器证书的请求。





图 13.8　申请服务器证书

13.5.3　申请服务器证书

首先打开浏览器，在地址栏中输入 http://ip/certsrv，其中 IP 地址为证书服务器的地址。在出现如图 13.9 所示的页面后，选中“申请证书”，然后单击“下一步”按钮。

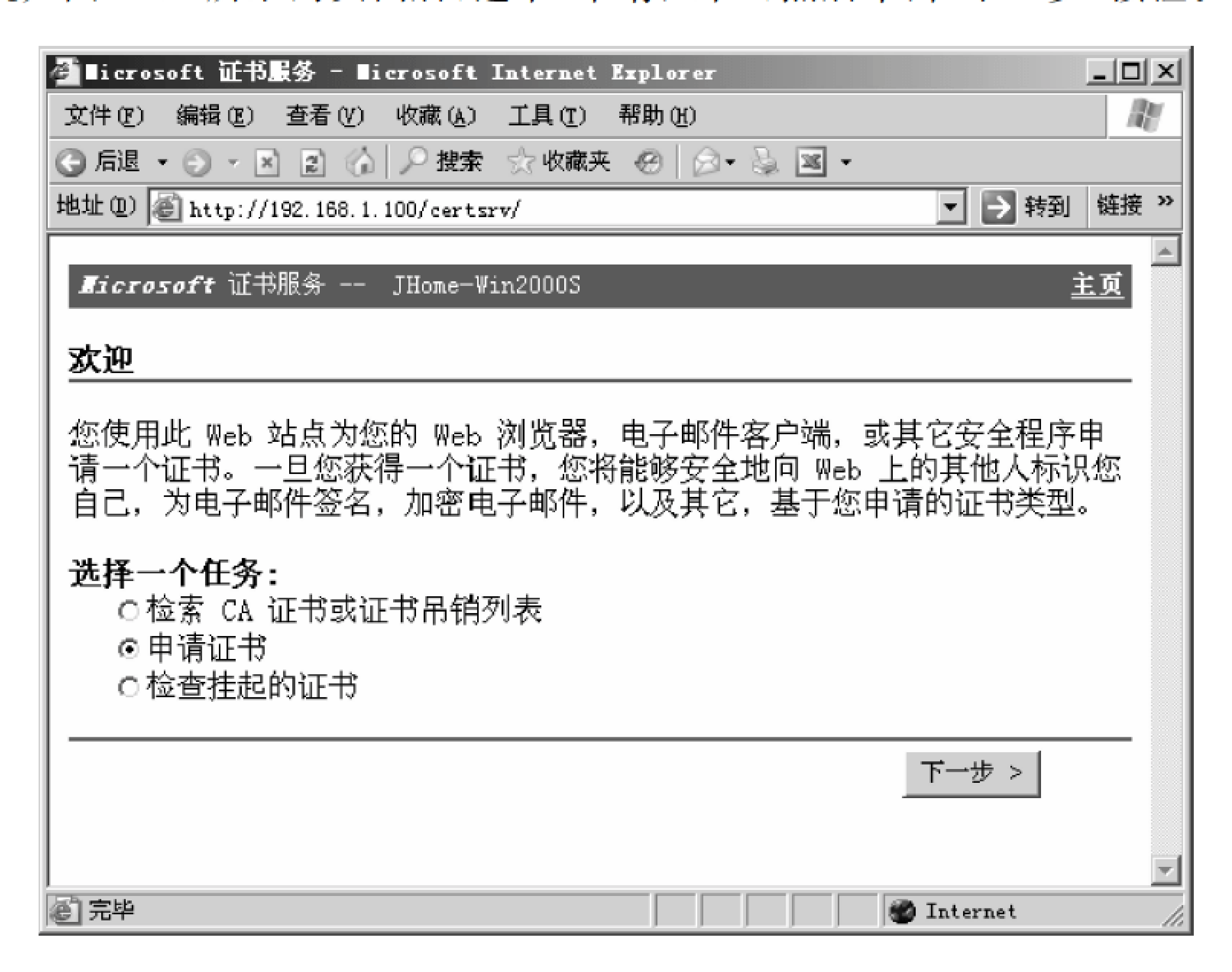


图 13.9　申请服务器证书

在出现的“选择申请类型”页面中，选中“高级申请”，并单击“下一步”按钮，如图 13.10 所示。



图 13.10 选择“高级申请”类型

在出现的“高级证书申请”页面中，选中中间的选项，如图 13.11 所示，然后单击“下一步”按钮。

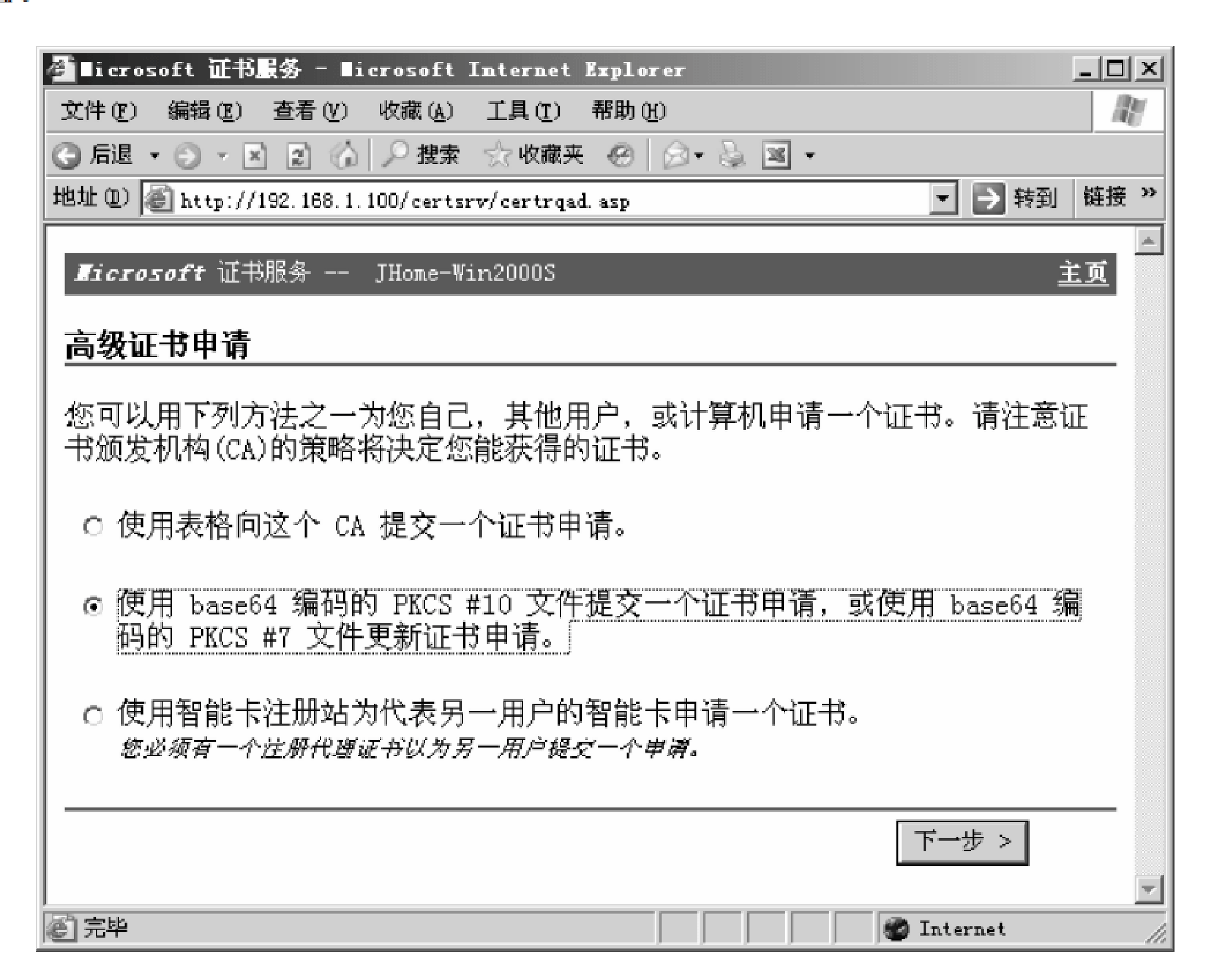


图 13.11 选择高级证书申请方式

打开文件 c:\certreq.txt，并将其内容复制到如图 13.12 所示的文本框中，然后单击“提交”按钮。

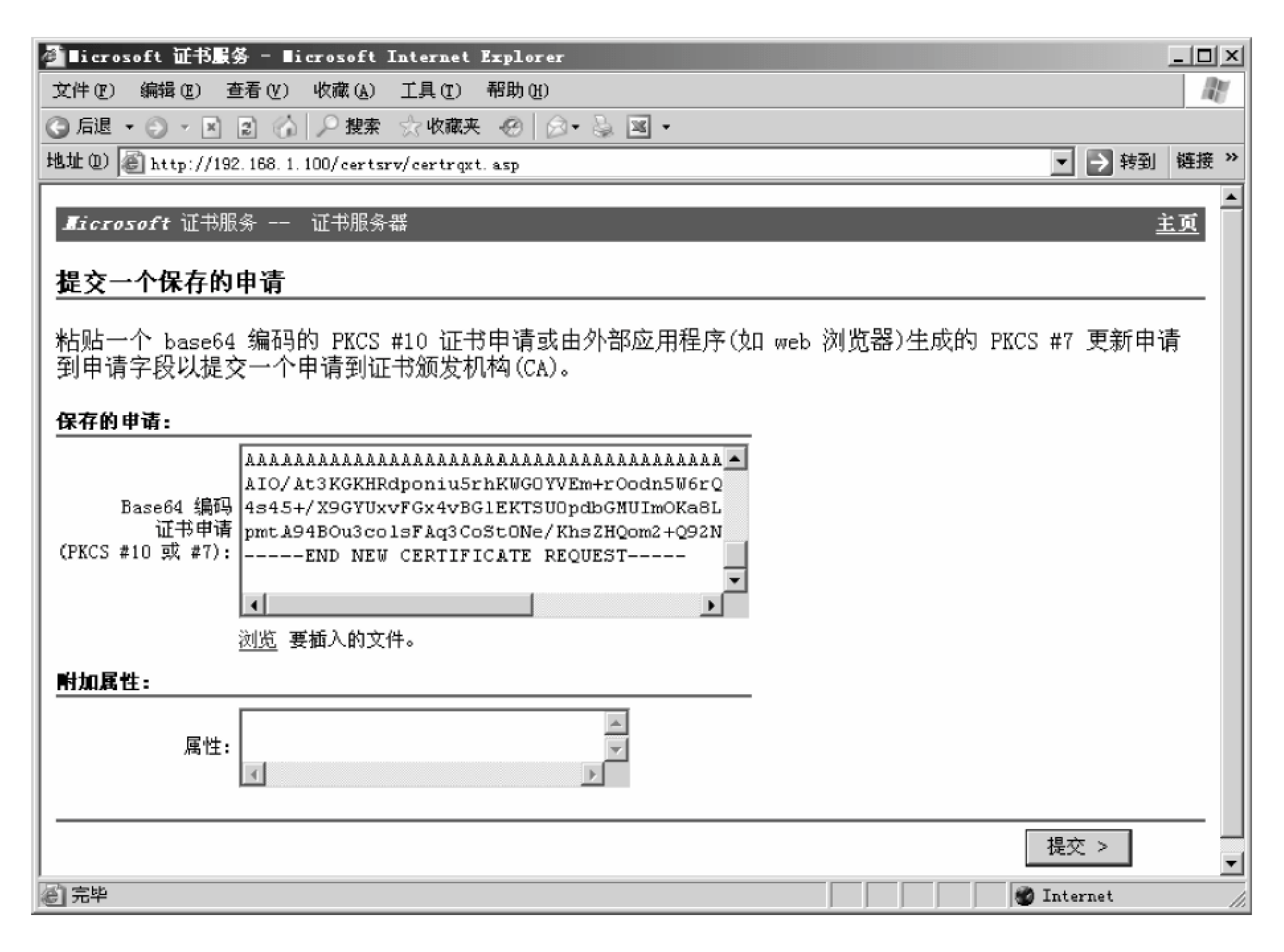


图 13.12 提交服务器证书申请

至此,就完成了 IIS 服务器证书的申请工作。

13.5.4 证书颁发

在证书管理服务器中,选择“开始”→“所有程序”→“管理工具”→“证书颁发机构”命令,打开证书管理界面,如图 13.13 所示。在该图的左边,单击“待定申请”。



图 13.13 “证书颁发机构”窗口

右键单击名为“2”的证书，在弹出的快捷菜单中选择“所有任务”→“颁发”，如图 13.14 所示。



图 13.14　颁发 IIS 服务器证书

在安装有 IIS 服务器的机器中，打开浏览器，并输入 http://ip/certsrv，打开证书服务页面，此时会出现如图 13.15 所示的界面。

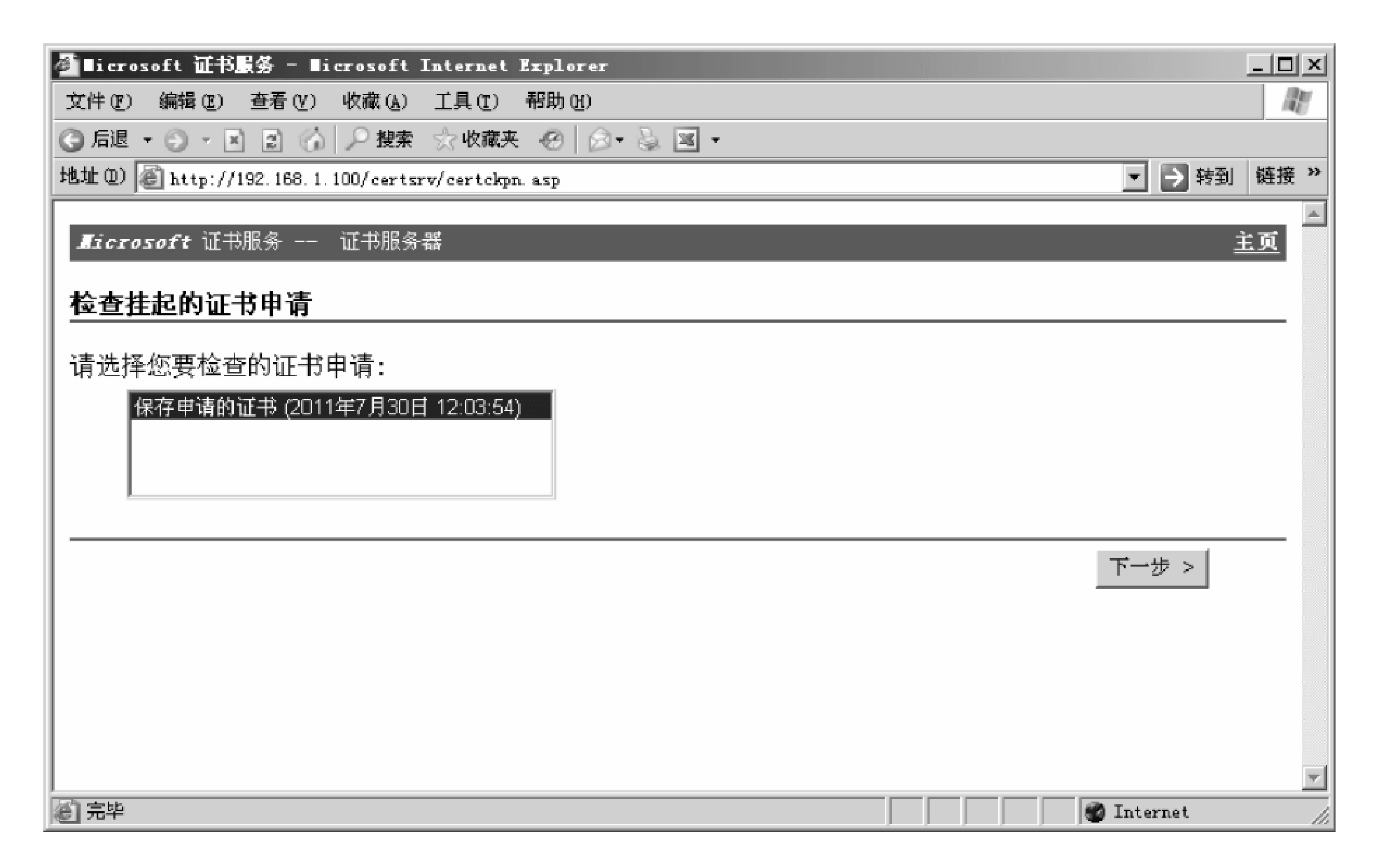


图 13.15　挂起的证书申请

选择“保存申请的证书”，并单击“下一步”按钮，将申请的证书下载并保存到本地硬盘上。

通过上述步骤，便获得了一个用于安装在 IIS 中的服务器证书。

13.5.5 证书安装

配置服务器证书的过程如下。

选择“开始”→“程序”→“管理工具”→“Internet 服务器管理”命令。

选择“默认站点属性”→“目录安全性”,在弹出的如图 13.16 所示对话框中选中“处理挂起的请求并安装证书”单选按钮。

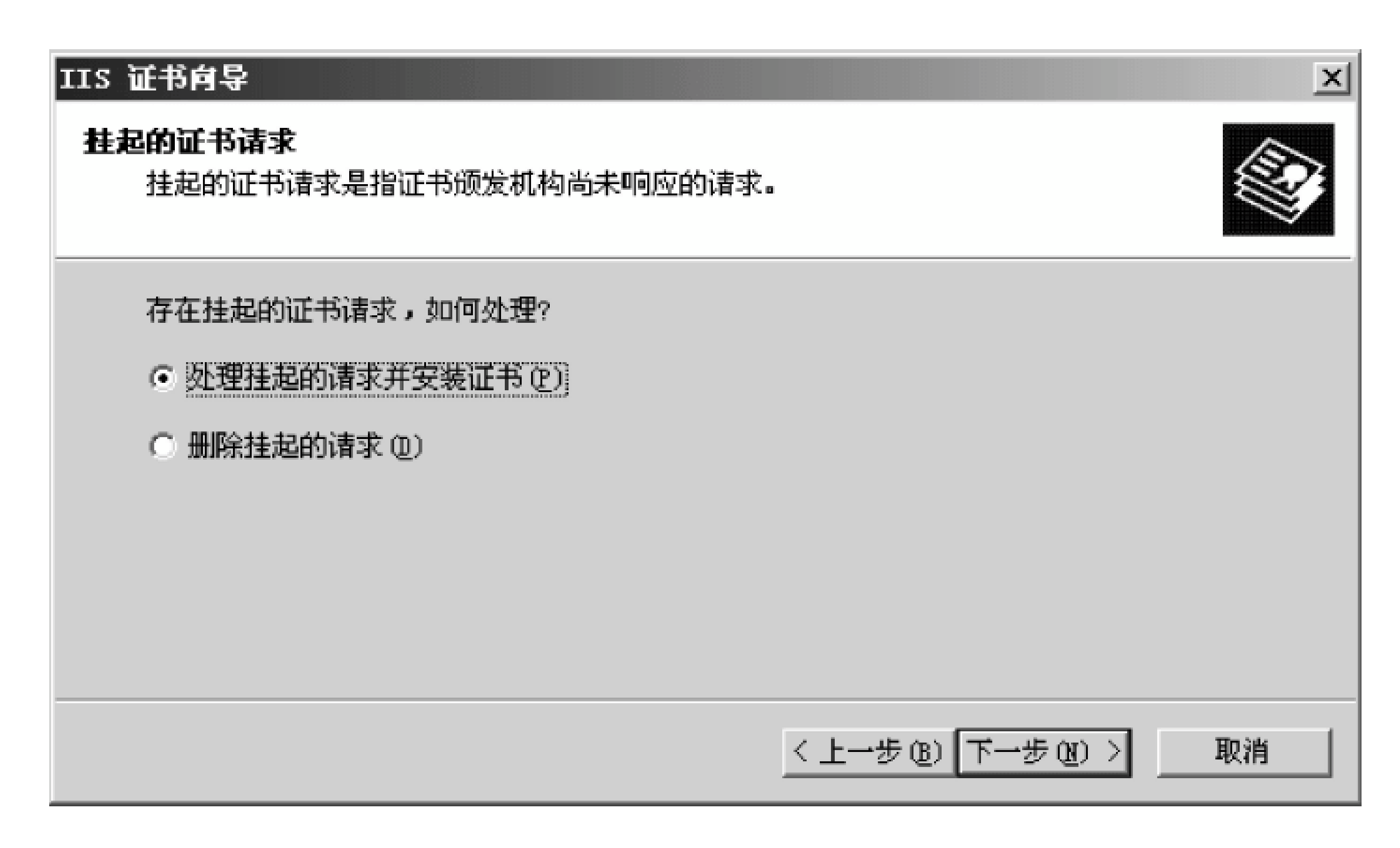


图 13.16 处理挂起证书请求

单击“下一步”按钮,在出现的如图 13.17 所示的对话框中单击“浏览”按钮,在弹出的“文件管理”对话框中选择在 13.5.4 节中下载的证书文件。单击“下一步”按钮,完成服务器证书的安装。

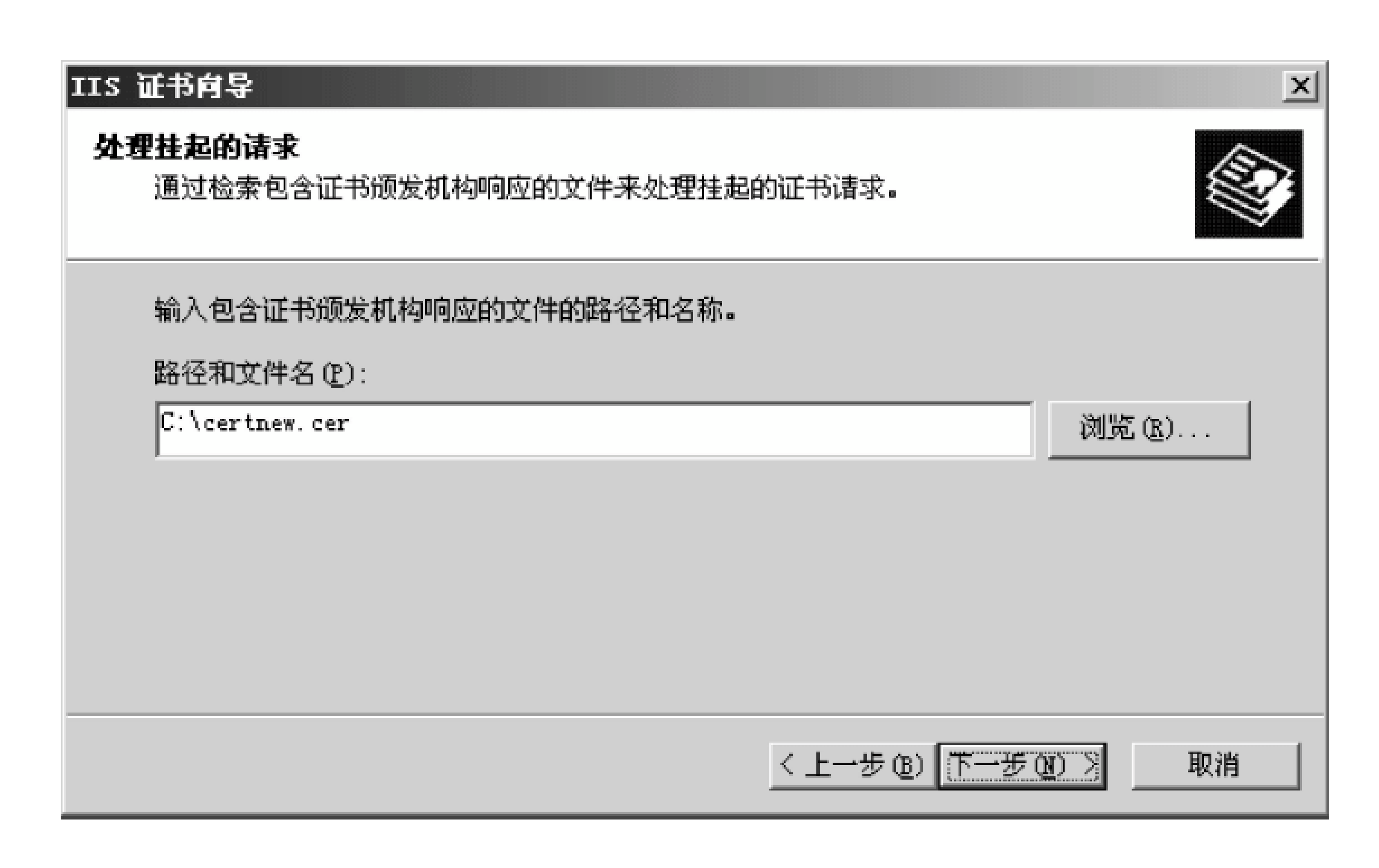


图 13.17 安装服务器证书

13.5.6 配置 IIS 中的 SSL

选择“开始”→“程序”→“管理工具”→“Internet 服务器管理”命令,单击“默认 Web 站

点”，在弹出的快捷菜单中选择“属性”→“目录安全性”→“编辑”，如图 13.18 所示，选中“要求安全通道（SSL）”复选框。



图 13.18 配置 SSL

13.5.7 测试 SSL

首先打开文本编辑软件，输入内容为 SSL 测试页面，然后将该页面另存为名为 default.html 的页面文件，如图 13.19 所示，并将该文件复制到 C:\Inetpub\wwwroot 目录下，覆盖掉同名文件。

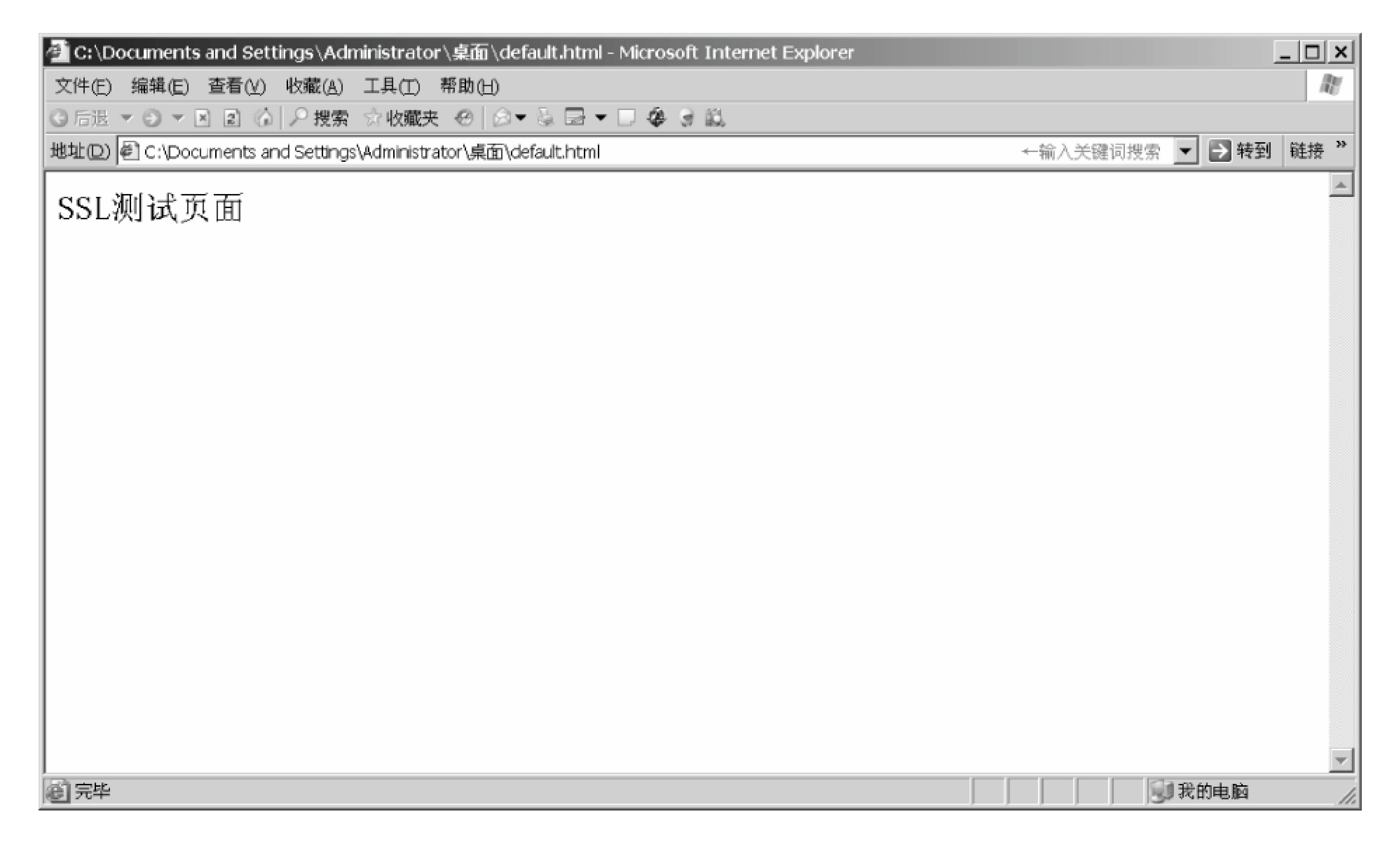


图 13.19 自定义的 default.html 文件

打开 IE 浏览器,输入 http://127.0.0.1/default.html,会出现如图 13.20 所示错误,错误提示要求使用 https 协议。

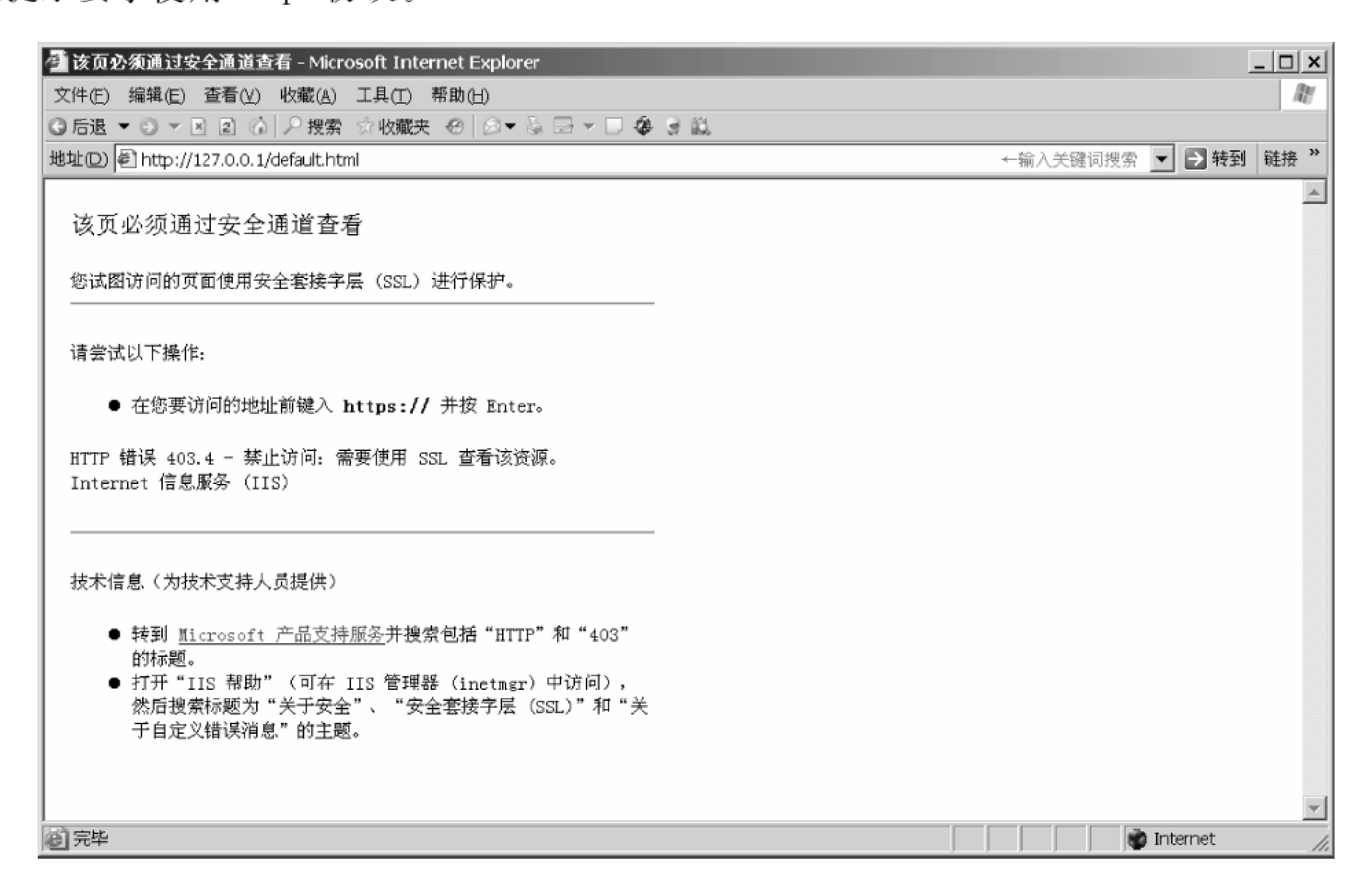


图 13.20 非 SSL 的 Web 访问

在地址栏中输入 https://127.0.0.1/default.html,出现如图 13.21 所示的安全警报。

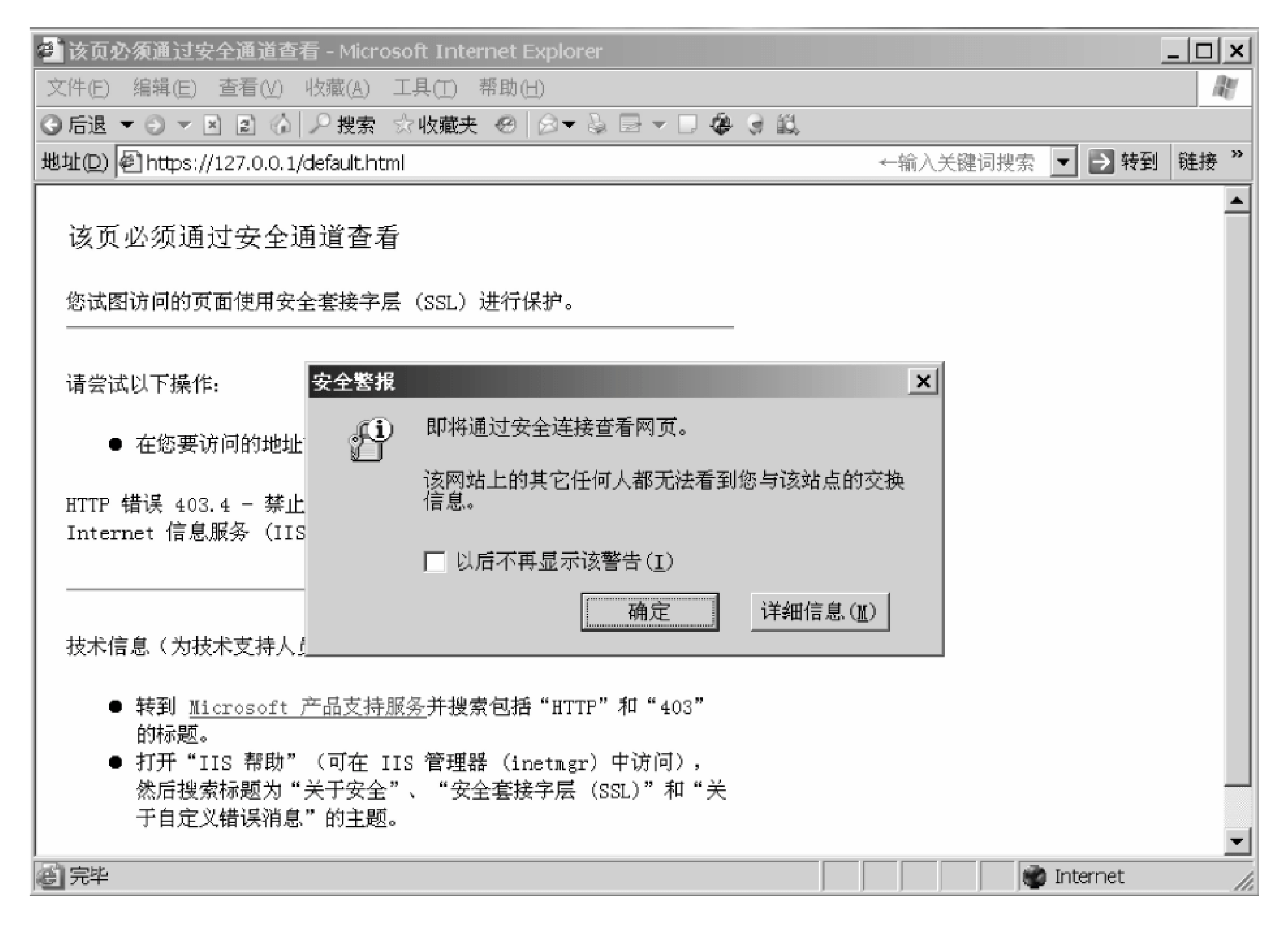


图 13.21 安全警报

单击“确定”按钮，则会显示出正常的SSL连接下的页面，如图13.22所示。

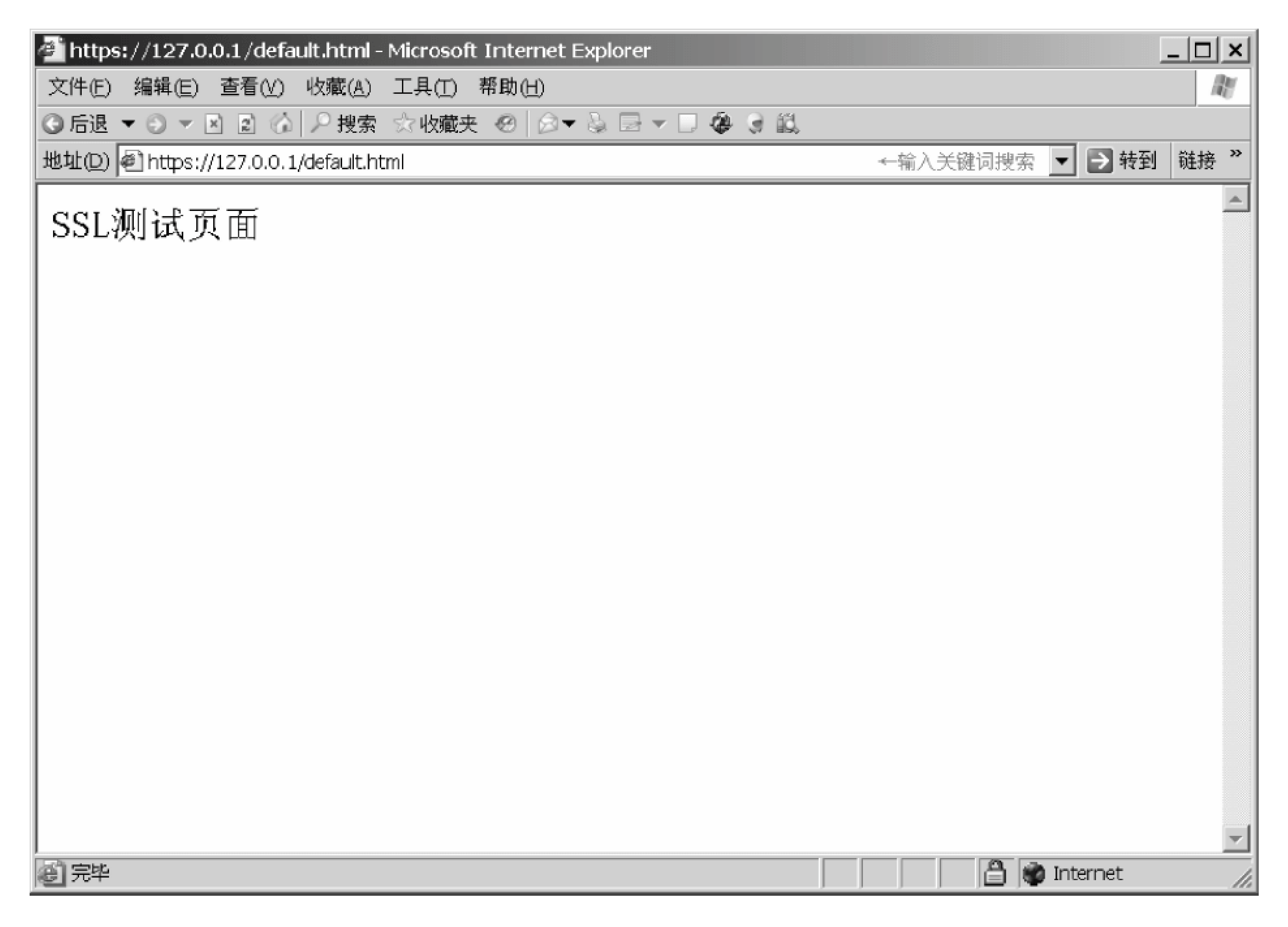


图13.22 SSL下的Web连接

13.6 实验思考

(1) 通过实验验证一下，如果不申请IIS服务器证书，能否在IIS中配置SSL协议？

(2) 利用实验9掌握的网络嗅探手段，验证能否从SSL连接中嗅探出有效的信息。

第 3 篇

攻击体会篇

ARTICLE 3



Windows 账户与口令破解

14.1 实验目的与要求

- 通过使用工具 LophtCrack 检测本地计算机的弱登录密码。
- 进一步理解账户与口令的安全性问题。

14.2 实验环境

- Windows XP 操作系统。
- 实验工具 LophtCrack 5.0。

14.3 预备知识

14.3.1 身份认证机制

操作系统的安全机制主要体现在身份认证和访问控制两个方面。身份认证(authentication)是证明某人或某个对象身份的过程,是保证系统安全的重要措施。身份认证需要用一个标识(identification)来表示用户的身份。将用户标识和用户联系的过程称为认证。操作系统的许多保护措施大都基于认证系统的合法用户,身份认证是操作系统中相当重要的一个方面,也是用户获取权限的关键。

操作系统中用户身份认证通常采用账户/口令的方案。账户是一种参考上下文,操作系统在这个上下文描述符运行它的大部分代码。换一种说法,所有的用户模式代码在一个用户账户的上下文中运行,即使是那些在任何人都没有登录之前就运行的代码(例如服务)也是运行在一个账户(特殊的本地系统账户 SYSTEM)的上下文中的。如果用户使用账户凭据(用户名和口令)成功通过了登录认证,之后他/她执行的所有命令都具有该用户的权限。于是,执行代码所进行的操作只受限于运行它的账户所具有的权限。恶意黑客的目标就是以尽可能高的权限运行代码。那么,黑客首先需要"变成"具有最高权限的账户。

口令是一种容易实现并有效地只让授权用户进入系统的方法。口令是用户与操作系统之间交换的信物。用户如果使用系统,首先必须通

过系统管理员向系统登录，在系统中建立一个用户账户，账户中存放用户的名字（或标识）和口令。用户输入的用户名和口令必须和存放在系统中的账户/口令文件中的相关信息一致才能进入系统。没有一个有效的口令，入侵者要闯入计算机系统是很困难的。账户/口令的认证方案普遍存在着安全的隐患和不足之处，具体有如下几种。

- 认证过程的安全保护不够健全，登录的步骤没有进行集成和封装，而是暴露在外，容易受到恶意入侵者或系统内部特洛伊木马的干扰或者截取。
- 口令的存放与访问没有严格的安全保护。
- 认证机制与访问控制机制不能很好地相互配合和衔接，使得通过认证的合法用户进行有意或无意的非法操作的机会大大增加。

14.3.2 SAM（Security Accounts Manager）

在使用 NT 内核的操作系统（Windows 2000/XP/2003/Vista）中，负责用户账户名和口令管理的模块被称为“安全账户管理器”（Security Accounts Manager），也就是通常所说的 SAM。

操作系统的所有账户、权限分配信息和密码都存储在 SAM 里，而 SAM 是以两个文件的形式保存在系统中的，即位于 SYSTEM32\CONFIG 目录里的 SAM 和安全辅助文件 security。这两个文件通过系统注册表 HKEY_LOCAL_MACHINE\SAM 的数据项来访问（SAM 组成了注册表的 5 个配置单元之一）。当修改用户账户信息时，此项会产生变化，而修改的结果就保存在 SAM 文件之中。SAM 记录的数据很多，包括所有组、账户信息、密码 HASH、账户 SID 等。SAM 里面存储的用户密码是一个使用“签名算法”产生的不可逆哈希值（Hash），而不是使用可逆算法生成的密码数据，因此 SAM 的账户密码是不能真正破解的（尽管如此，散列的口令是可以被猜出的）。

在 Windows 2000 域控制器上，用户账户和哈希值的数据保存在活动目录中（默认为%systemroot%\ntds\ntds.dit）。哈希值是以相同的格式保存的，但是要访问它们必须通过不同的方法。默认情况下管理员无权访问 SAM 数据库，要查看它使用 RegEdt32 修改 SAM 访问权限，或者使用 psu、wsu 启动 system 权限的 regedit。

在整个 SAM 数据库中，账户主要内容存在于下面这些位置：

在\Domains\下就是域（或本机）中的 SAM 内容，其下有两个分支“Account”和“Builtin”。\Domains\Account 是用户账户内容，\Domains\Account\Users 下就是各个账户的信息。其下的子键就是各个账户的 SID 相对标识符。比如 000001F4，每个账户下面有两个子项，F 和 V。其中\Names\下是用户账户名，每个账户名只有一个默认的子项，项中类型不是一般的注册表数据类型，而是指向标志这个账户的 SID 最后一项（相对标识符），比如其下的 Administrator，类型为 0x1F4，于是从前面的 000001F4 就对应着账户名 administrator 的内容。由此可见 Windows 账户搜索的逻辑。

仍然使用上面的例子：\Domains\Account\Users\000001F4 中存放的是 administrator 的账户信息（其他类似），其中有两个子项 V 和 F。项目 V 中保存的是账户的基本资料，用户名、用户全名（full name）、所属组、描述、密码 hash、注释、是否可以更改密码、账户启用、密码设置时间等。项目 F 中保存的是一些登录记录，比如上次登录时间、错误登录次数等，

还有一个重要的地方就是这个账号的 SID 相对标志符。本实验中多次涉及到项目 V 中的密码 hash。

14.3.3 L0phtcrack 5.0 密码测试工具

1. 简介

L0phtcrack 5.0,简称 LC5,是一种用于审计和恢复 Windows 操作系统和 UNIX 操作系统用户口令的有力工具。借助于 LC5,系统管理员能够全面审计 Windows NT、Windows 2000、Windows XP、UNIX 系统中用户登录密码的强度,维护系统安全;同时,还能够恢复被遗忘的用户登录密码。

LC5 不仅可以恢复本地计算机用户的登录密码,而且可以恢复远程计算机用户的登录密码。在恢复本地计算机的登录密码时,LC5 的使用者需要具有本地计算机管理者的权限;在恢复远程计算机的登录密码时,LC5 的使用者需要具有远程计算机管理者的权限。此外,LC5 还可以恢复出 SAM 文件中被加密的密码,以及通过网络嗅探得到的网络中被加密的密码。

LC5 恢复密码的方式有 4 种,即快速密码审计、普通密码审计、强力密码审计与自定义密码审计。其中,快速密码审计需要几分钟时间依次将 LC5 自带的一个字典中的每一个明文加密后与待测的密码密文相匹配。若匹配成功,则恢复出相应的密码。这种方式适于恢复较为简单的密码。普通密码审计则是依靠内置程序自动地改变字典中一定数量的字符,形成新的字典序列,从而用以恢复较为复杂的密码。强力密码审计则是通过穷举所有的数字、字符和特殊字符,形成明文字符串,加密后与待恢复的密码密文相匹配,从而能够发现更为复杂的密码,然而这种恢复方式时间较为漫长。而自定义方式则按照用户的需求构造明文字典,然后用于恢复密码。

L0phtCrack 能直接从注册表,文件系统,备份磁盘,或是在网络传输的过程中找到口令。L0phtCrack 开始破解的第一步是精简操作系统存储加密口令的 hash 列表,之后才开始口令的破解,这个过程称为 cracking。它采用 3 种不同的方法来实现。

(1) 最快也是最简单的方法是字典攻击。L0phtCrack 将字典中的词逐个与口令 hash 表中的词作比较。当发现匹配的词时,显示结果,即用户口令。L0phtCrack 自带一个小型词库。如果需要其他字典资源可以从互联网上获得。这种破解的方法,使用的字典的容量越大,破解的结果越好。

(2) 另一种方法名为 hybrid。它是建立在字典破解的基础上的。现在许多用户选择口令不再是单单由字母组成的,他们常会使用诸如“bogus11”或“Annaliza!!”等添加了符号和数字的字符串作为口令。这类口令是复杂了一些,但通过口令过滤器和一些方法,破解它也不是很困难,Hybrid 就能快速地对这类口令进行破解。

(3) 最后一种也是最有效的一种破解方式“暴力破解”。按道理说真正复杂的口令,用现在的硬件设备是无法破解的。但现在所谓复杂的口令一般都能被破解。只是时间长短的问题;且破解口令时间远远小于管理员设置的口令有效期。使用这种方法也能了解一个口令的安全使用期限。

2. 怎样得到口令的 hash 列表

开始破解过程，L0phtCrack 首先需要检索口令 hash 列表。如果用户有管理权限，可以使用 Tools Dump Passwords from Registry 命令在 L0phtCrack 菜单上检索 hash 表。用户可以从本地机上或是允许访问的远程机倒出口令 hash 列表。在注册表对话框中的 Dump Passwords 输入 NT 机器名，或 IP 地址，单击 OK 按钮。用户名和密码下载到 L0phtCrack 中。对口令列表的检索结束之后，开始执行口令过程。

第二种是通过文件系统访问 hash 列表。因为操作系统对 SAM 文件进行了加密，口令存储在该文件系统中。当操作系统在运行过程中，是不可能从文件系统中得到任何信息的。有时候，文件系统的备份被保存在磁盘或一个加密的 repaire 磁盘上或是在系统硬件的 repair 目录上。同时，其他的操作系统(如 DOS 系统)可以从软盘启动，口令 hash 能直接从文件系统得到。如果用户能对计算机进行物理访问，这种方法很有用。

用户可以从“SAM”或“SAM.-”文件中下载 hash 列表到 L0phtCrack，这可通过使用 FileImport SAM File 菜单命令下载指定的 hash 列表来实现。L0phtCrack 将自动在 NT 上展开“SAM”文件(注意：如果用户使用的是 Win 95/98，展开“SAM.-”文件到“SAM”，使用在 NT 系统的扩展指令。该命令是 expand sam.-sam.)。

L0phtCrack 提供的最后一种获得 hash 列表的方法是通过网络。用户的机器一定有一个或多个以太网设备对网络进行访问。使用 Tool SMB Packet Capture 命令启动 SMB 包捕获窗口。网络设备能获得任何 SMB 认可的部分。如果用户转换网络，就只能看到本机或连接的机器原有的任务。当 SMB 认可的任务授权被捕获时，在 SMB Packet Capture 的窗口显示。内容有：源代码、目的 IP 地址、用户名、SMB 口令、加密 LAMMAN hash 列表和加密 NTLM hash 列表等。Save Capture 命令保存捕获到的信息，用来破解 hash 表。File Open Password 命令打开捕获的内容。同时，还可以对其他的口令进行捕获和破解。

Todd Sabin 已经发布了一个免费的工具，能在本地导出口令的 hash 列表。如果 SAM 使用的是 SYNKEY 工具进行加密(该资源在 Service Packet3 中有介绍，可从 http://www.webspan.net/～pwdump2 中得到)，根据网站上的指导可以对口令的 hash 表进行检索。用户可以使用 File Open Password File 命令下载 hash 列表到 L0phtCrack 中。

3. 如何破解口令 hash 列表

L0phtCrack 的第一种方法是使用字典攻击。该方法通过使用字典中的词库进行破解工作。将词库中的所有的口令与口令 hash 列表作比较。如果得到了匹配的词，则破解成功。L0phtCrack 自带了一个有 25 000 个词的名为 words-english 的文件，其中包括了许多常见的作为口令的词。也可用 File Open Qordlish 文件菜单命令下载其他的字典到 L0phtCrack。

开始破解的过程：选择菜单上的 Tools Run Crack。默认的方法顺序是字典攻击、hybrid 攻击、暴力破解。通常在使用了这 3 种方法之后，L0phtCrack 大都能成功地获得口令。如果用户愿意也可以在 Tools Option 对话框中定义破解攻击的具体步骤。

L0phtCrack 窗口显示的状态信息表明，字典攻击成功的概率和字典中词库的大小成正

比例。

在字典攻击失败后，开始 Hybrid 攻击。Hrbrid 使用简单的模式，用户通过对一般词汇的改变产生的口令进行攻击。L0phtCrack 能智能化地尝试口令的猜测。比如试一试“BOGUS11”。许多的用户仅仅在一些原有词的基础上添加了很少的数字或符号，来试图创造一个不可猜测的口令。但 L0phtCrack 能很快猜测出这些口令，而不再需要进行暴力攻击。L0phtCrack 的 Hybrid 的破解方法，使用的默认检验字符或数字的个数是 2。也可以通过 Tools Options 命令来改变该数值。

在字典攻击和 hybrid 攻击失败之后，就是暴力攻击。它可能会消耗相当长的时间，但是这些时间远远小于口令的有效期。因此这些口令在暴力攻击面前显得格外的脆弱。可以通过使用“Tool Option”命令改变字符数字的设置。默认的设置是尝试所有的数字和字符。

在 Pentium II/450 到 Pentium 166 的 CPU 上理想的暴力破解时间是应该 24～72 小时。

14.4 实验内容

本章的实验内容主要包括以下两部分：

（1）演示如何利用 Windows 系统自带的“本地安全设置”来制定高强度的密码以及保护密码的安全设置。

（2）演示如何利用 LC5 软件来测试密码的强度。

14.5 实验步骤

14.5.1 利用密码策略强制设置高强度密码

本节实验内容参见实验 6 的 6.5.2 节。

14.5.2 保护密码安全策略的设置

1. 设置密码长度最小值

设置密码长度最小值有助于防止用户设置过短的密码，避免用户密码被轻易猜出。单击“开始”→“运行”，在“运行”窗口中输入：secpol.msc，单击“确定”按钮，则打开了“本地安全设置”对话框。在该对话框的左侧单击“账户策略”，然后在右侧双击“密码策略”→“密码长度最小值”，则打开了该项策略的设置，如图 14.1 所示。



图 14.1 设置密码长度最小值

一旦该策略生效，再次更改密码时，则必须

符合该策略中设置的密码长度,否则会提示错误。

2. 密码最长存留期与密码最短存留期

设置密码最长存留期可提醒用户在经过一定时间后更改正在使用的密码,这有助于防止长时间使用固定密码带来的安全隐患。设置密码最短存留期不仅可避免由于高频繁地更改密码带来的密码难以使用的问题(如由于高度频繁地更改密码导致用户记忆混乱),而且可防止黑客在入侵系统后更改用户密码。

双击“本地安全设置”中的“密码策略”→“密码最长存留期”,则打开了该项策略的设置,如图 14.2 所示。以类似的方式,可以进行“密码最短存留期”的设置。

3. 强制密码历史

“强制密码历史”安全策略可有效防止用户交替使用几个有限的密码所带来的安全问题。该策略可以让系统记住用户曾经使用过的密码。若用户更改的新密码与已使用过的密码一样,系统会给出提示。该安全策略最多可以记住 24 个曾使用过的密码。双击“本地安全设置”中的“密码策略”→ “强制密码历史”,则打开了该项策略的设置,如图 14.3 所示。



图 14.2 设置密码最长存留期



图 14.3 设置强制密码历史

注意:为了使“强制密码历史”安全策略生效,必须将“密码最短存留期”的值设为一个大于 0 的值。

4. 账户锁定策略

账户锁定策略可发现账户操作中的异常事件,并对发生异常的账户进行锁定,从而保护账户的安全性。打开“本地安全设置”窗口,在窗口左侧依次选择“账户策略”→“账户锁定策略”,则会看到该策略有三个设置项:“复位账户锁定计数器”、“账户锁定时间”、“账户锁定阈值”,如图 14.4 所示。

“账户锁定阈值”可设置在几次登录失败后就锁定该账户。这能有效防止黑客对该账户密码的穷举猜测。当“账户锁定阈值”的值设定为一个非 0 值后,则可以设置“复位账户锁定计数器”和“账户锁定时间”两个安全策略的值。其中“复位账户锁定计数器”设置了计数器复位为 0 时所经过的分钟数;“账户锁定时间”设置了账户保持锁定状态的分钟数,当时间过后,账户会自动解锁,以确保合法的用户在账户解锁后可以通过使用正确的密码登录系统。

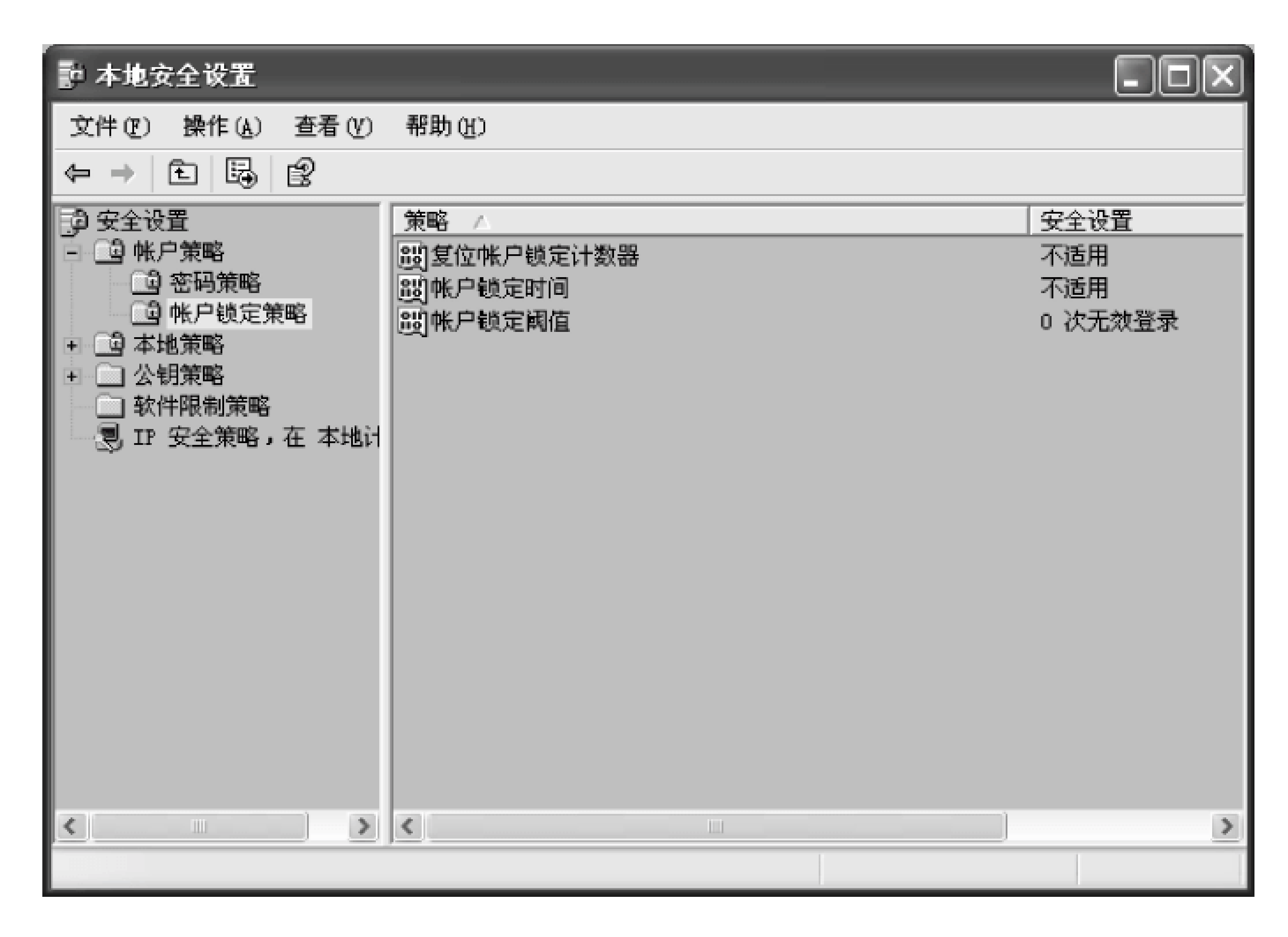


图 14.4 账户锁定策略

当“账户锁定阈值”设置为一个非 0 值后，“复位账户锁定计数器”与“账户锁定时间”会自动设置为默认值，如图 14.5 所示。默认值可在这两个安全策略中分别修改。



图 14.5 “复位账户锁定计时器”与“账户锁定时间”的默认值

5. 重命名管理员账户

用户登录系统的账户名对于黑客来说也有着重要意义。当黑客得知账户名后，可发起有针对性的攻击。目前许多用户都在使用 Administrator 账户登录系统，这为黑客的攻击创造了条件。因此我们可以重命名 Administrator 账户，使黑客无法针对该账户发起攻击。

打开“本地安全设置”窗口，在窗口左侧依次选择“安全设置”→“本地策略”→“安全选项”，如图 14.6 所示。在窗口右侧双击“账户：重命名系统管理员账户”选项，在弹出的对话框中将更改 Administrator 账户名，如图 14.7 所示。

14.5.3 使用 LC5 测试密码

① 使用 Net User 命令创建用户 Tuser1、Tuser2 和 Tuser3，登录密码分别设置成简单的大写字母 ABCDEFG、小写字母 abcdefg 和数字 1234567，如图 14.8 所示。



图 14.6　打开“安全选项”



图 14.7　重命名管理员账户

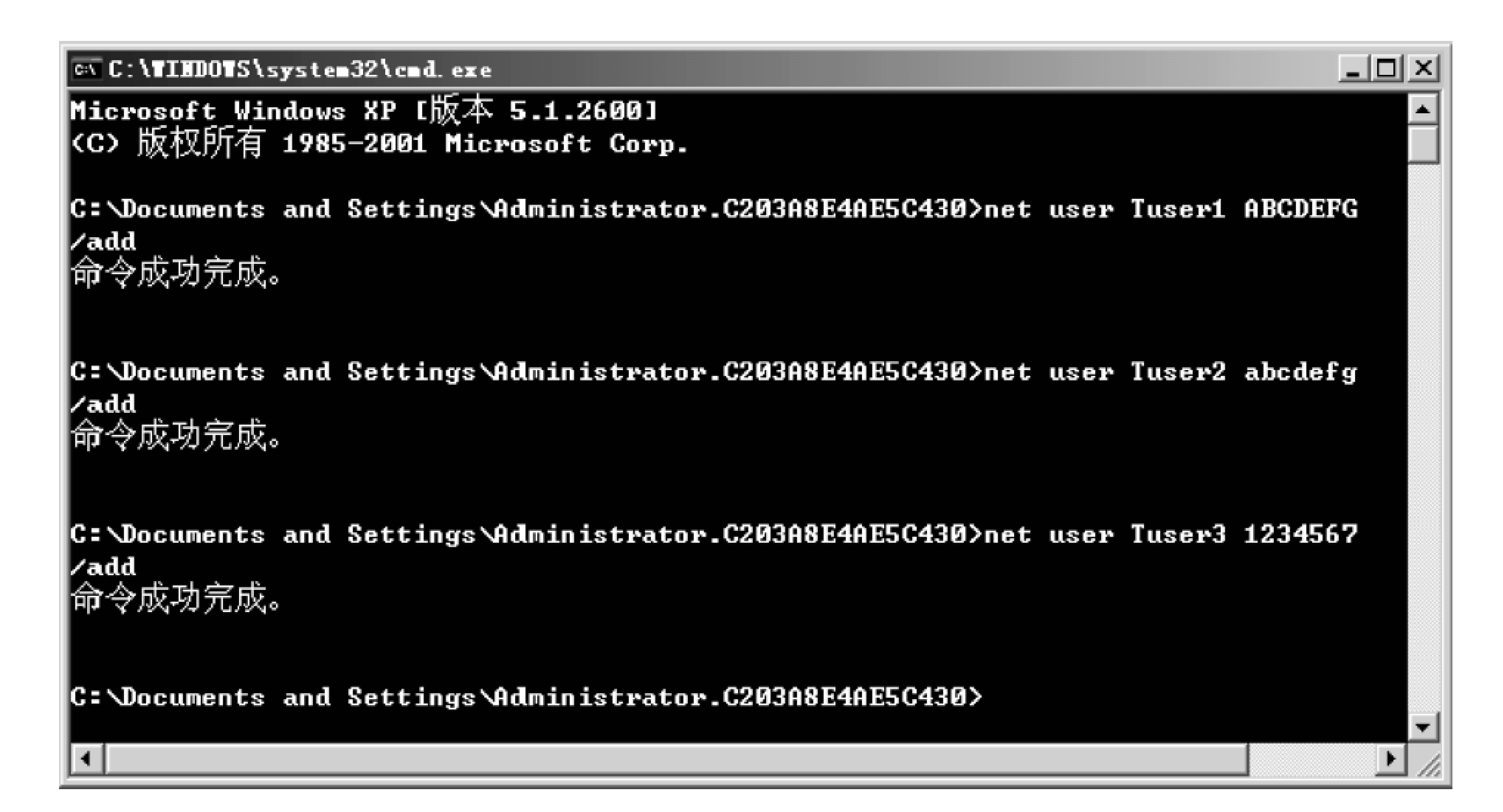


图 14.8　添加用户账户

② 从开始菜单中启用 LC5，在弹出的 LC5 Wizard 对话框中单击“下一步”按钮，如图 14.9 所示。

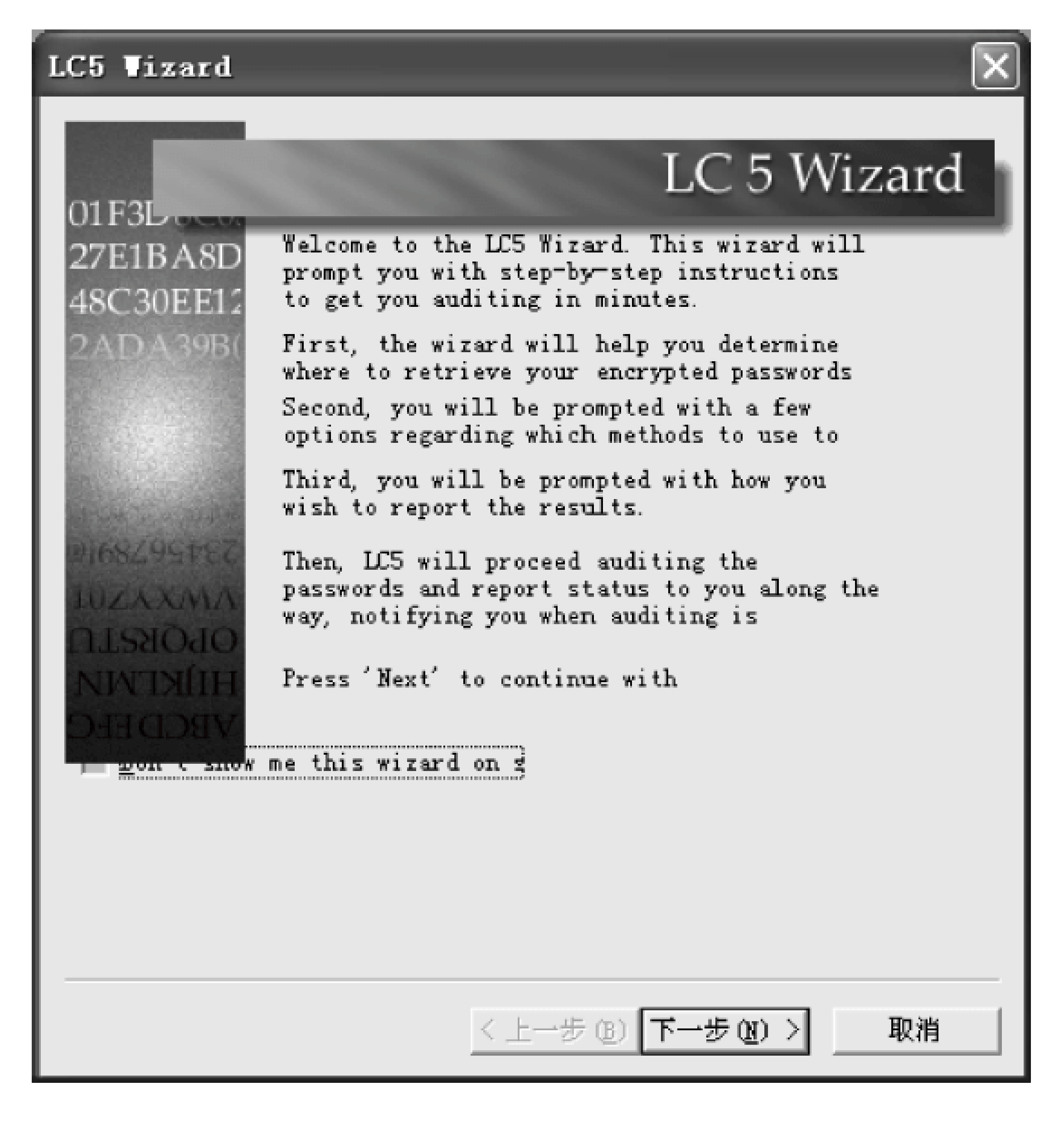


图 14.9　启动 LC5

③ 因为要恢复本地用户的登录密码，因此在弹出的 Get Encrypted Passwords 对话框中选择第一项“Retrieve from local machine”，单击“下一步”按钮，在 Choose Auditing Method 对话框中选择 Quick Password Audit，然后按照提示操作，最后在出现的主窗口中看到 3 个用户的登录密码已显示出来，如图 14.10 所示。

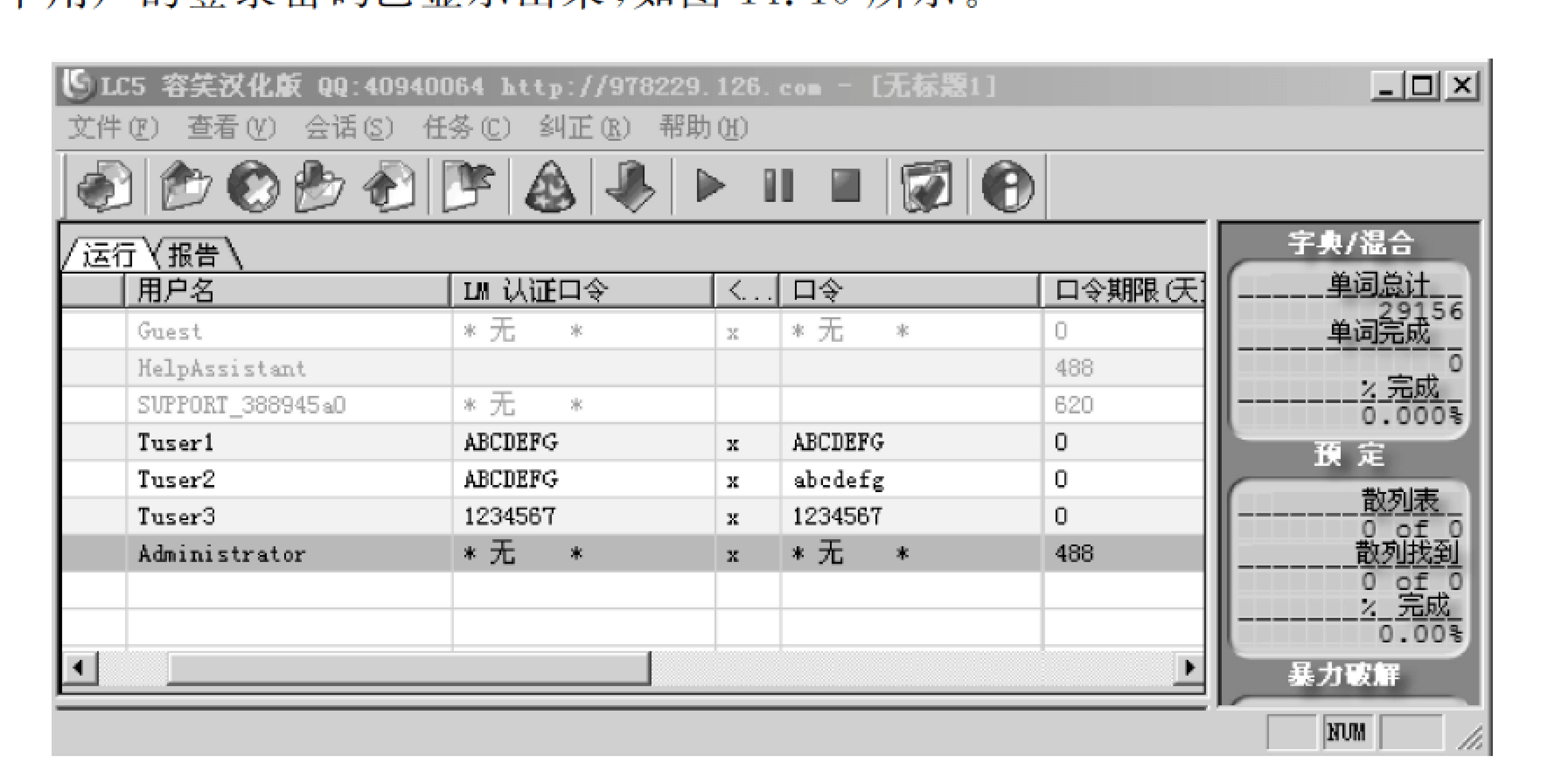


图 14.10　简单密码的恢复

④ 使用 Net User 命令修改用户密码，设置成较复杂的组合密码，如 Tuser1 的新密码为 abcdEFG，Tuser2 的新密码为 abcd123，Tuser3 的新密码为 ABCD123，如图 14.11 所示。



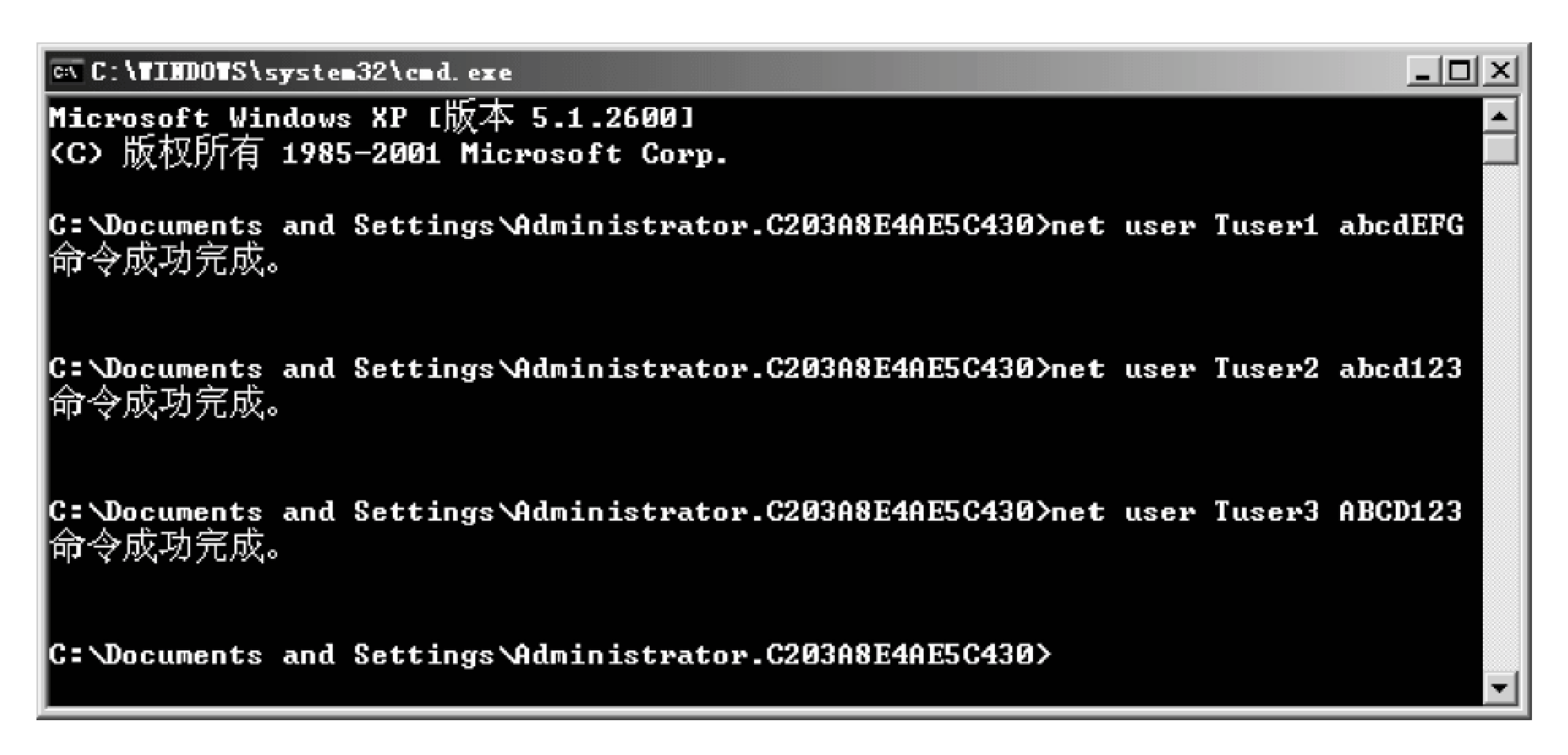


图 14.11　设置较复杂的组合密码

⑤ 重新启动 LC5，选择 Quick Password Audit 选项进行密码恢复，可发现在该选项下 LC5 在较短的时间内能够破解所有简单组合的登录密码，如图 14.12 所示。

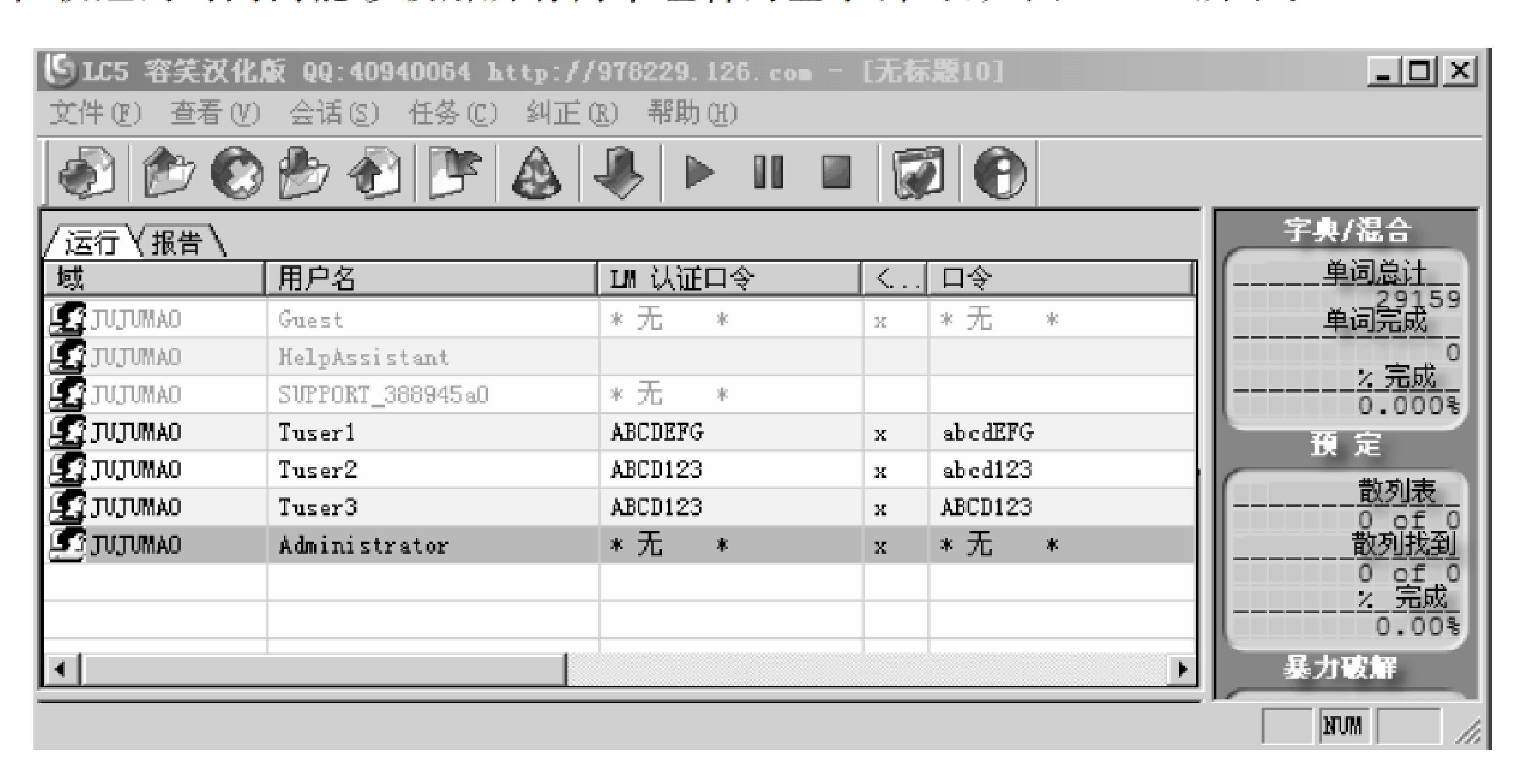


图 14.12　组合密码的恢复

⑥ 使用 Net User 命令修改用户 Tuser1 的密码，设置成复杂的大小写字母、数字与特殊字符组合 12ab#AB，启用工具 LC5，在 Strong Password Audit 的选项下实施密码恢复，如图 14.13 所示。

可以看到图中右下角显示“暴力破解”的进度，所花费时间越长，则说明密码强度越高。

⑦ 再来看一下 Windows 系统关于密码位数分组的问题。将用户口令设置成大于 7 个字符的复杂密码，Tuser1 为 12ab#AB，Tuser2 为 12ab#ABC，Tuser3 为 12ab#ABCD。启用工具 LC5，可以看到密码的后两位立刻被恢复，而前 7 位密码短时间内没有被恢复出来，如图 14.14 所示。这说明在 Windows 系统中，密码是按 7 个字符进行分组的。

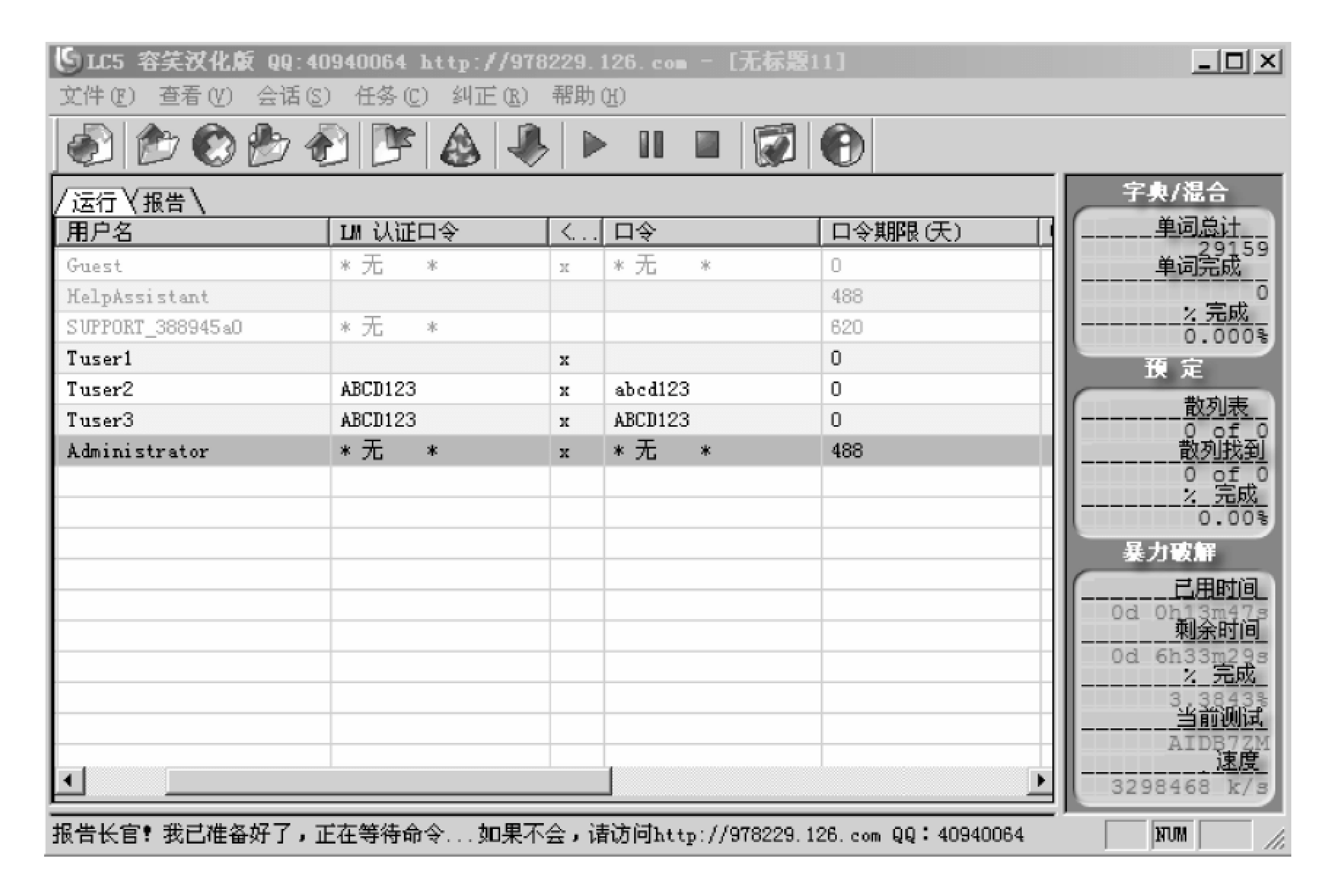


图 14.13 复杂密码的恢复

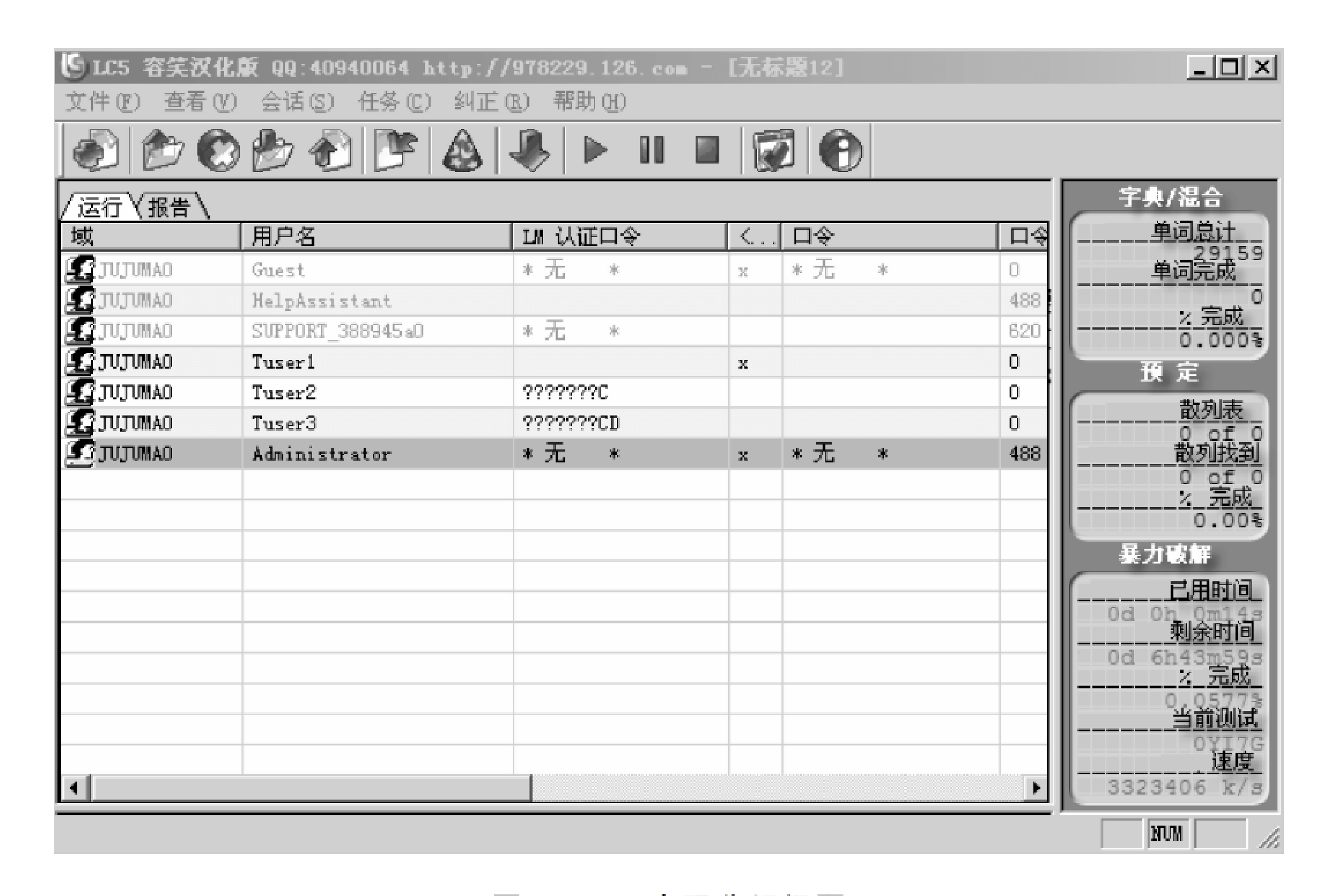


图 14.14 密码分组问题

14.6 实验思考

(1) 尝试在 Windows 7 系统下打开“本地安全设置”对话框(与 Windows XP 系统不同)。

(2) 思考仅使用登录密码来保护系统会存在什么样的安全隐患。

实验15 ARP 攻击实验

15.1 实验目的与要求

- 了解 ARP 的概念以及 ARP 攻击的原理。
- 采取有效措施对 ARP 攻击进行防范。

15.2 实验环境

- 一个小型局域网环境。
- 在局域网的一台 Windows XP 系统上安装 ARP 攻击器 3.5。

15.3 预备知识

1. ARP 定义

当以太网中的两台设备需要直接通信时，必须知道对方的 MAC 地址，因此，数据包在以“帧”的形式向外传播时，必须首先得到对方的 MAC 地址。而 ARP 协议就是一种能够将目的 IP 地址解析成目的 MAC 地址的数据链路层协议。该协议的工作就是在主机发送数据帧之前，通过广播目的 IP 地址来查询目的 MAC 地址，从而保证通信的顺利进行。

2. ARP 攻击原理

ARP 攻击就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞，攻击者只要持续不断地发出伪造的 ARP 数据包就能更改目标主机 ARP 缓存中的 IP-MAC 条目，造成网络中断或中间人攻击。

伪造的 ARP 数据包具有如下的特点：

(1) 伪造的 ARP 数据包中，源 MAC 地址/目的 MAC 地址和以太网帧封装中的源 MAC 地址/目的 MAC 地址不一致。

(2) 伪造的 ARP 数据包中，源 IP 地址和源 MAC 地址的映射关系不是预定的合法的映射关系。

基于伪造的 ARP 数据包,可以发起如下几种常见的 ARP 攻击。

(1) 伪造网关攻击。进行 ARP 欺骗的主机 A 通过将网关的 IP 地址和自身的 MAC 地址相绑定,伪造出 ARP 数据包,导致局域网内的其他主机相信 A 的 MAC 地址为网关地址,从而将发送给网关的数据包错误地发送给主机 A,从而造成正常的数据不能被网关接收。如果主机 A 是通过广播的方式发送伪造的 ARP 数据包,将会造成整个局域网的通信中断。因此,这是一种对于局域网比较严重的攻击。

(2) 伪造用户欺骗网关攻击。进行 ARP 欺骗的主机 A 将主机 B 的 IP 地址与 A 的 MAC 地址相绑定,从而伪造出 ARP 数据包,并发送给网关。这将导致网关的 ARP 数据表中记录了错误的关于主机 B 的 IP-MAC 地址映射。这将导致主机 B 不能正常地接收来自网关的数据包。

(3) 伪造用户欺骗局域网内其他用户。进行 ARP 欺骗的主机 A 将主机 B 的 IP 地址与 A 的 MAC 地址相绑定,从而伪造出 ARP 数据包,并发送给主机 C,这将导致 C 的 ARP 数据表中记录了错误的关于主机 B 的 IP-MAC 地址映射,还将导致主机 B 不能正常地接收来自主机 C 的数据包。

(4) ARP 洪泛攻击。由于主机处理 ARP 数据包时需要消耗系统资源,因此主机一般会限定 ARP 表的大小。利用这一点,攻击者可以伪造大量的具有新 IP 地址的 ARP 数据包,导致主机设备在将这些 ARP 数据包加入 ARP 表时,造成 ARP 表溢出,并导致合法的 ARP 数据包无法加入 ARP 表,从而导致整个局域网的通信中断。

3. 对 ARP 攻击的防御

ARP 工具对于局域网环境有着很大威胁,因此必须采取一些措施来提高网络的安全性。

(1) 建立静态 ARP 缓存表。所谓 ARP 的欺骗攻击就是通过更改主机上缓存的动态 IP-MAC 对应表来达到欺骗主机的目的。使用静态的 IP-MAC 对应表将 IP 地址与 MAC 地址进行静态绑定,则可以有效地解决 ARP 欺骗问题。

例如,可以建立如下的文件:

```
www.sdfi.edu.cn09:00:20:ab:a1:e2
oa.sdfi.edu.cn 09:00:20:dd:ad:1g
```

然后使用 ARP f filename 命令将其加载到 ARP 表中,这样添加的 ARP 映射将不会过期和被新的 ARP 数据刷新,只能使用 ARP d 命令进行删除。

但是这种方法破坏了动态的 ARP 协议,一旦合法主机的网卡地址改变后,就必须手工刷新 ARP 表。因此,这种方法不适合于经常变动的网络环境。

(2) 禁止 ARP。可以通过 ipconfig interface-ARP 命令来完全禁止 ARP,这样,网卡将不会发送 ARP 和接收 ARP 数据包。但前提是使用静态 ARP 表,否则计算机将不能通信。这个方法并不适用于大多数网络环境,因为它增加了网络管理的成本。但是对小规模的安全网络而言,还是有效可行的。

15.4 实验内容

本章的实验内容是以 BanGaTeway 攻击为例，来演示如何操作 ARP 攻击器来对局域网的计算机实施攻击。

15.5 实验步骤

首先，单击 ARP 攻击器的 Scan 按钮，会在下方列出局域网内所有机器的列表，如图 15.1 所示。

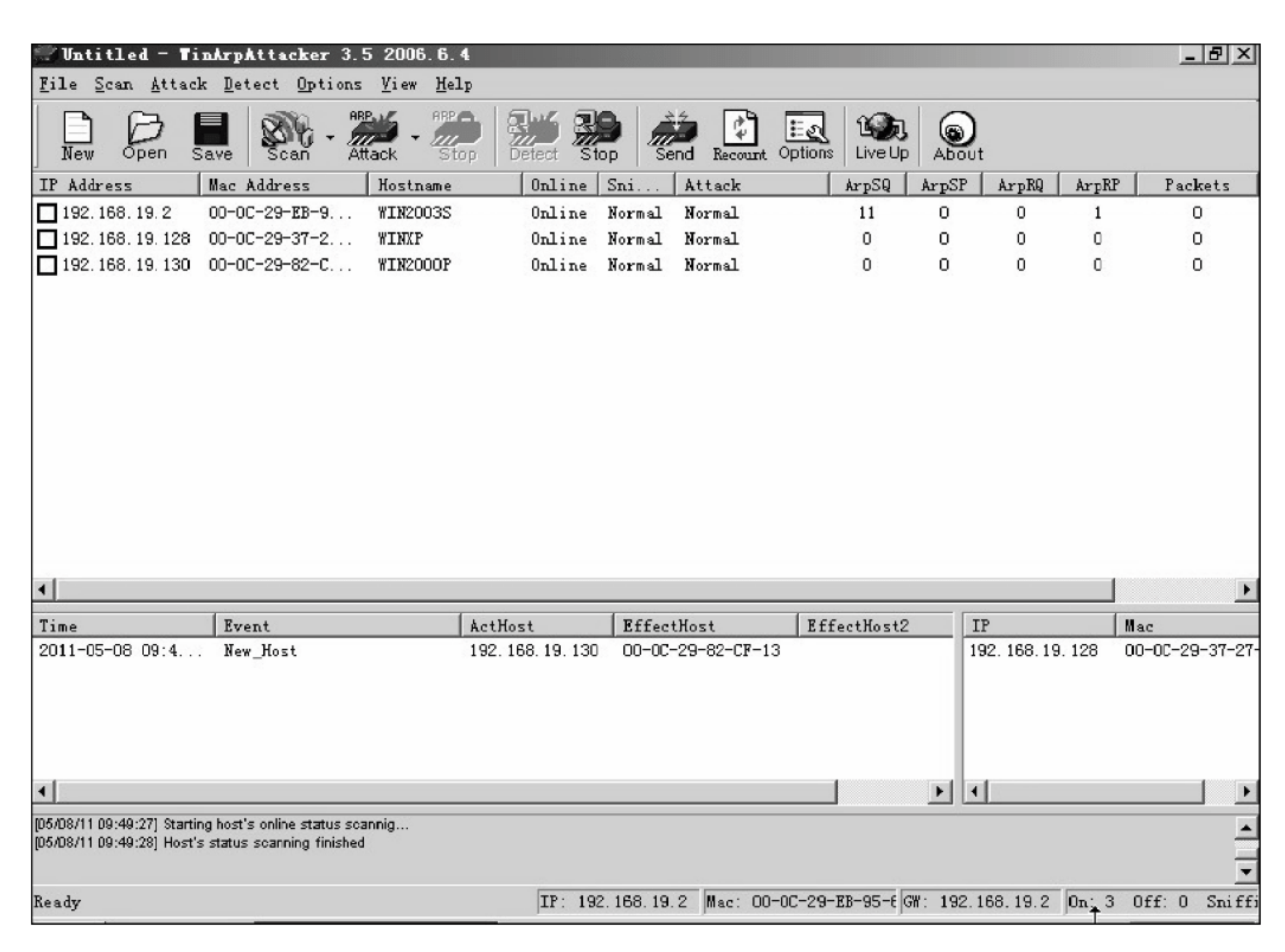


图 15.1 扫描局域网

在图 15.1 所示的列表中选择要进行 ARP 攻击的目标计算机，单击 Attack 下拉按钮，会出现 6 种攻击方式，如图 15.2 所示，它们的功能如下：

- Flood　不间断的 IP 冲突攻击。
- BanGaTeway　禁止上网。
- IP Conflict　定时的 IP 冲突。
- Sniff Gateway　监听选定机器与网关的通信。
- Sniff Hosts　监听选定的几台机器之间的通信。

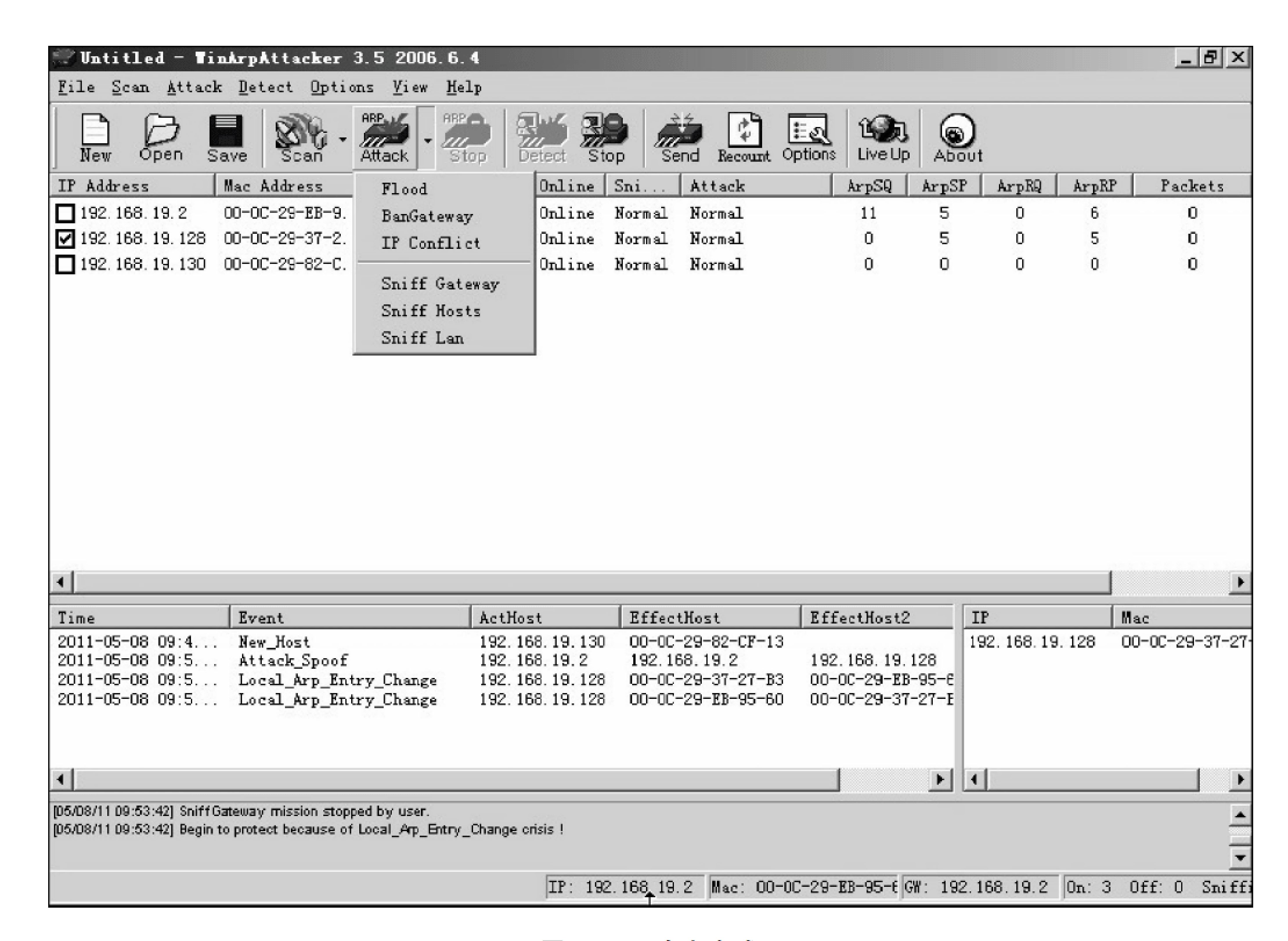


图 15.2 攻击方式

- Sniff Lan　监听整个网络任意机器之间的通信，这个功能过于危险，可能会把整个网络搞乱，建议不要乱用。

各个攻击的作用如下。

(1) Flood。选定主机，在攻击中选择 Flood 攻击，Flood 攻击默认是一千次，可以在选项中改变这个数值。Flood 攻击可使对方主机弹出 IP 冲突对话框，导致宕机，因此要小心使用。

(2) BanGaTeway。选定主机，选择 BanGaTeway 攻击，可使对方机器不能上网。

(3) IPConflict。会使对方机器弹出 IP 冲突对话框。

(4) SniffGateway。监听对方主机的上网流量，发动攻击后用抓包软件来抓包看内容，可以看到 Packets、Traffic 两个统计数据正在增加。

(5) SniffHosts、SniffLan 与 SniffGateway 类似。

单击要使用的攻击方式即可开始攻击，攻击效果如图 15.3 所示。

通过图 15.3 可以看出，IP 地址为 192.168.19.128 的计算机其 MAC 地址被替换成了错误的 MAC 地址，这将导致该计算机无法接收来自网关的数据包，从而导致该计算机无法正常上网。

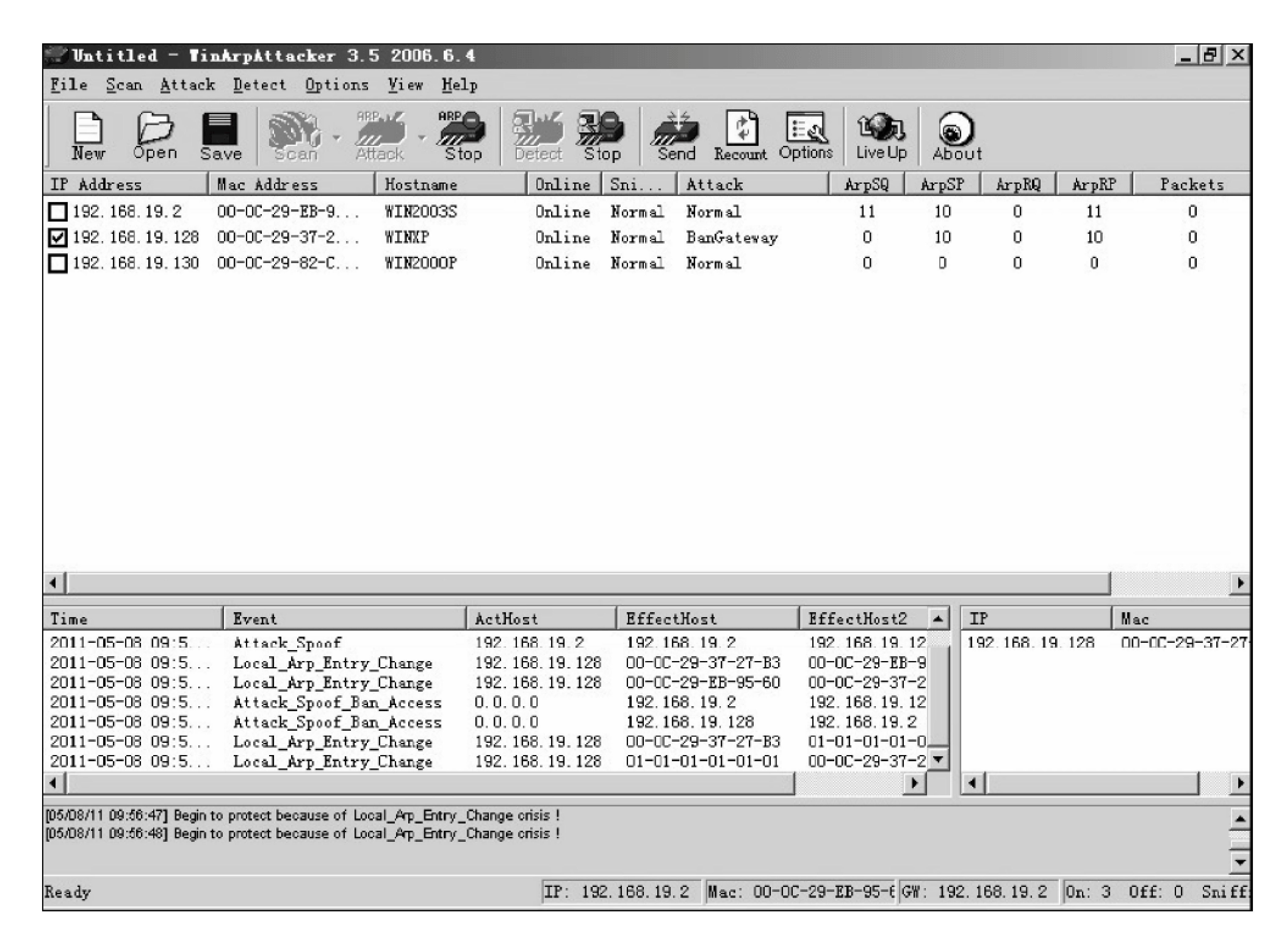


图 15.3 实施 ARP 攻击

15.6 实验思考

(1) 在本地计算机上建立静态 ARP 缓存表,并通过实验来验证这种方法对 ARP 攻击的防御效果,并思考这种方法的不足之处。

(2) 在本地计算机上禁用 ARP,并通过实验来验证这种方法对 ARP 攻击的防御效果,同时思考这种方法的不足之处。

实验16 远程控制实验

16.1 实验目的与要求

- 了解远程控制的概念及原理。
- 提高远程控制防范的意识。

16.2 实验环境

- 两台 PC,分别将 IP 地址设置为 192.168.1.182(控制端)和 192.168.1.183(被控制端),确保两者可以通信。
- 在控制端 PC 上安装灰鸽子软件。

16.3 预备知识

1. 远程控制

远程控制技术是由网络上的一台计算机(客户端/监控方)去访问和控制网络上另一台计算机(服务器端/被监控方)的技术。该技术一般在局域网范围内实施,但也能用于广域网。当一个用户使用远程控制技术控制网络上的另一台计算机时,该用户所使用的计算机被称为客户端,而被控制的计算机被称为服务器端,即客户端计算机可以访问服务器端计算机上的信息,并能够利用服务器计算机上的资源(如文件、CPU、内存、声卡、显卡)实施某种操作。如此一来,该用户就如同坐在被监控计算机的屏幕前,可以启动被监控计算机的应用程序,读取、修改和执行其中的文件,甚至可以利用其外联的打印机和通信设备进行打印和互联网的访问。

远程控制技术的核心是通过将主控计算机上的键盘和鼠标指令传递给远程的计算机,并在该计算机上执行。这种技术在以下一些领域发挥着重要的作用:

- 远程技术支持。专业技术人员可以远程控制用户的计算机,从而便捷地发现用户计算机上存在的问题,并及时加以解决。

- 远程维护。网络管理人员可以通过远程控制的方式为用户计算机进行合理的配置、下载安装软件和补丁等。
- 远程交流。商业公司可以采用交互式的教学模式实现和用户的远程交流,通过远程控制在用户端实现的本地实际操作来培训用户。
- 远程办公。既使工作人员远离工作环境,也能通过远程控制的方式进行办公。

在实现远程控制技术时,必须在远程的计算机系统上安装一个服务器端软件,而在主控计算机上安装一个客户端软件,而远程控制就是通过客户端软件访问服务器端软件来实现的。如果一台计算机通过某种方式被安装了一个服务器软件,那么该计算机很可能会被拥有相应客户端软件的计算机所控制,此时,该服务器软件又可称为"木马"。

木马一般具有如下特征。

- 隐蔽性。即服务器端软件能够在被监控的计算机上很好地隐藏自己,如木马不会产生一个图标。
- 欺骗性。为了隐藏自身,木马往往会采用欺骗的手段,如利用"1"和"l"的相似性以及"0"和"o"的相似性来伪造一些不易被区分的文件名来欺骗计算机的使用者。
- 自动运行。当系统开始运行后,木马则开始运行。
- 打开端口。木马必须在被监控的计算机上打开一个端口,以便让远程的客户端软件进行访问。一般而言,木马不会占用系统端口号,而是使用 1024 以上的端口。如果我们知道该端口号,并把该端口关掉,那么即使木马能够运行,也不会产生破坏作用。

2. 灰鸽子软件

自 2001 年灰鸽子软件诞生起,它就以丰富而强大的功能,灵活多变的操作和良好的隐蔽性而受到世人的关注。当合法使用时,该软件是一款优秀的远程控制软件,而当被非法使用时,其就成为了一款强大的黑客远程控制工具。目前,灰鸽子多用于黑客工具,其变种多达数万种,对社会的网络信息安全构成了极大的威胁。

16.4 实验内容

本章的实验内容主要包括两部分:

(1) 演示如何对灰鸽子远程控制软件进行配置,包括控制密码的设置和服务器端程序的生成。

(2) 演示如何利用灰鸽子远程控制软件对远程计算机进行控制。

16.5 实验步骤

首先在监控 PC 上打开灰鸽子程序,如图 16.1 所示。

然后单击图 16.1 中的"配置服务程序"按钮,开启"服务器配置"对话框,进行服务器程序的配置,如图 16.2 所示。

在图 16.2 中的"IP 通知 http 访问地址、DNS 解析域名或固定 IP"中填入在攻击成功后



图 16.1 打开"灰鸽子"程序

图 16.2 "服务器配置"对话框

如何通知客户端的方式。单击"说明"按钮，在弹出的对话框中有各种方式的示例方式，局域网环境中，一般填入监控 PC 的 IP 地址即可。这样，被监控 PC 中的信息将会由 IP 地址指定的 PC 进行控制。

在图 16.2 中，单击"上线图像"旁的左右键按钮可以调整当被监控 PC 上线时的头像；在"上线分组"可以填写被监控 PC 上线时的分组（也可默认）；在"上线备注"中可填写被监控 PC 上线时显示的备注（也可不填）；在"连接密码"中可填写在线控制被监控 PC 时的访问密码（如不设则为空），以防止别的监控 PC 对被监控 PC 进行控制；在"历史配置记录"中存储了以前服务器程序的配置情况；在"保存路径"中，可以设置生成的服务器端程序将要保存的路径以及所要保存的名称；当设置完成后，单击"生成服务器"按钮，将会弹出"提示信息"对话框，显示配置成功，如图 16.3 所示。

当服务器程序产生后，可以通过其他手段对服务器程序进行一些适当的处理，如免杀、夹克、捆绑等，尽量把服务器端伪装成一个良性的程序，然后可以将其上传到网站供别人下载运行或者通过其他欺骗的方式，如 QQ 传递等将其传递给远程的 PC 运行。当远程 PC 运行配置好的服务器程序时，则立即成为被监控 PC。

图 16.3 "配置服务器程序成功"信息框

在监控 PC 上打开灰鸽子程序，那么可以在图 16.4 左下方的"文件管理器"属性页下面的"文件目录浏览"里面出现了"暗组"并且显示出一条记录，在"连接密码"输入框中输入配置时设置的密码，如 123，单击旁边的"保存"按钮后，即可完成对被监控 PC 的控制（若密码输入错误，则无法完成对被监控 PC 的控制），如图 16.4 所示。此时，便可以在"文件目录浏览"下查看被监控 PC 上的文件内容。与"文件管理器"属性页并列的还有"远程控制命令"、"注册表编辑器"、"命令广播"三个属性页，可以单击它们，以对被监控 PC 进行有效的远程控制。

另外，单击图 16.4 上部工具栏中的"捕获屏幕"按钮，可以在被监控 PC 的用户不知情的情况下查看被监控 PC 的屏幕状态。



图 16.4 监控被控制的 PC

16.6 实验思考

（1）在灰鸽子软件中，为什么放在远程计算机上的程序称为服务器端程序？

（2）请思考如何防范由灰鸽子等远程控制软件带来的威胁。



Windows 映像劫持技术

17.1 实验目的与要求

- 理解映像劫持的概念和原理。
- 掌握处理映像劫持的方法。

17.2 实验环境

Windows XP 操作系统。

17.3 预备知识

所谓映像劫持，通常被称为"IFEO"，即 Image File Execution Options(映像文件执行选项)，但事实上，映像劫持是基于 IFEO 技术的一种针对应用程序的攻击手段，应被称为 IFEO Hijack。

1. IFEO

早期的 Windows NT 架构中，系统使用了一种称之为堆(heap)的管理机制。随着技术的发展，后来微软又引入了动态内存分配方案来改进基于堆的管理机制，从而让程序占用更少的内存，并在缓冲区溢出方面提高了安全性。但是这种改进方案却造成一些以早期设计模式运行的程序无法运行。为了保障这些程序在后继操作系统中的顺利运行，微软提供了 IFEO 机制，而后又对该机制进行了扩充，最终形成了一套可用于调试程序的简易方案。在这种调试方案中，IFEO 提供了 13 种与堆分配有关的参数，如 ApplicationGoo、PageHeapFlags 等。当一个应用程序处于 IFEO 的控制之下时，它的内存分配则由与该程序相对应的上述所列参数来控制。

为了将应用程序处于 IFEO 的控制之下，Windows NT 为用户提供了一个交互机制，其位于注册表的"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options"位置中。在这个位置，可以使用应用程序的文件名作为一个注册表项，并在其内容中来设置该程序的堆管理机制和一些辅

助机制。同时，为了调试方便，并减少注册表的冗余，IFEO 机制忽略了应用程序的存储路径，仅依靠文件名对该程序进行控制。比如，若 IFEO 要对 notepad. exe 进行控制，则只要在“HKEY _ LOCAL _ MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion\Image File Execution Options”下创建一个名为“notepad. exe”的注册表项即可，无论该程序处于哪个文件目录下，只要其文件名为“notepad. exe”，就会受到 IFEO 机制的控制。

2. IFEO Hijack

为了便于使用调试器对程序进行调试，微软在 IFEO 中实施了一种机制，即对应用程序配置一个 Debugger 参数，并可以通过直接运行某个应用程序的文件名来开启调试器对该应用程序进行调试。为了实现该机制，IFEO 将 Debugger 参数的优先级设置为最高，即如果系统发现某个应用程序的文件名 A 位于注册表的 IFEO 位置，当 A 运行时，它就会首先读取 Debugger 参数的值，若这个值不为空，那么系统就会把该值中指定的文件名 B 视为 A 的实际程序去运行，而把真正的文件名 A 仅仅作为 B 程序运行的一个参数。这就意味着通过 Debugger 参数，系统将用户运行程序 A 的请求重定向(redirection)到了应用程序 B。

利用 Debugger 参数的上述机制就可以实施一种映像劫持(IFEO Hijack)攻击(又称之为重定向攻击)。例如，注册表的 IFEO 位置有一个名为 notepad. exe 的注册表项，该注册表项 Debugger 参数的值为 c:\abc. exe，其中 abc. exe 为一个木马程序，其本身能够运行的同时，还可以通过传入参数来调用其他的程序运行。那么，当系统用户打开文本文档时，系统会首先根据 notepad. exe 文件的 Debugger 参数去运行 C:\abc. exe(即把 abc. exe 视为 notepad. exe 的调试器)，而“C:\windows\notepad. exe”则作为一个参数传递给了 abc. exe。这样一来，abc. exe 可以首先秘密开启木马程序，而后打开用户所需的 notepad. exe，这会造成系统在用户不知情的状态下感染木马。而如果木马 abc. exe 不能接受参数“C:\windows\nptepad. exe”，那么用户在打开文本文档时，可能会感觉系统没有任何反应，而事实上，系统已经在后台运行木马了。

3. IFEO Hijack 的处理方法

当在 Windows 操作系统中执行一个应用程序，而执行结果与预期相差比较大，比如说系统弹出提示信息，或者没有任何反应，则系统很可能被映像劫持攻击了。此时有以下几种可行的解决办法。

(1) 修改应用程序文件名。映像劫持是基于应用程序文件名的一种攻击，如果被劫持的应用程序为 A，那么只要将应用程序的名字 A 改为 B 即可绕过该攻击。这是因为，文件名 B 在注册表的 IFEO 位置没有相应的注册表项，所以系统就会到该应用程序的目录中去执行该文件，这样，映像劫持就不会发生了。

(2) 修改注册表。由于映像劫持攻击是通过在注册表的 IFEO 位置添加了一个以应用程序的文件名命名的注册表项，而后又对该注册表项添加了一个 Debugger 参数值来实现的。那么我们就可以进入注册表的“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\

Windows NT\CurrentVersion\Image File Execution Options”这个位置,并查看每个子项的 Debugger 参数是否有异常即可。另外,还可能存在注册表对应的应用程序 regedit.exe 和 regedt32.exe 被劫持的情况,此时,只要在 c:\windows 目录下修改 regedit.exe 和在 c:\windows\system32 目录修改 regedt32.exe 即可。

(3) 控制注册表的访问权。由于映像劫持攻击的实施需要修改注册表,那么只要提高用户访问注册表的权限,或者禁止对注册表的 IFEO 位置进行写入,均可有效制止映像劫持攻击。在下面的实验中,将对如何控制注册表的访问权进行介绍。

17.4 实验内容

本章的实验内容包括两部分:

(1) 演示利用注册表进行映像劫持攻击的方法。

(2) 演示如何通过对注册表设置访问权限的方法来预防映像劫持攻击。

17.5 实验步骤

17.5.1 映像劫持攻击

本实验使用 cmd.exe 来映像劫持 notepad.exe。

单击“开始”→“运行”命令,打开“运行”对话框,在其中输入 regedit,单击“确定”按钮,则打开了注册表编辑器。在注册表编辑器的左边一栏,按照“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options”展开到 IFEO 位置,如图 17.1 所示。

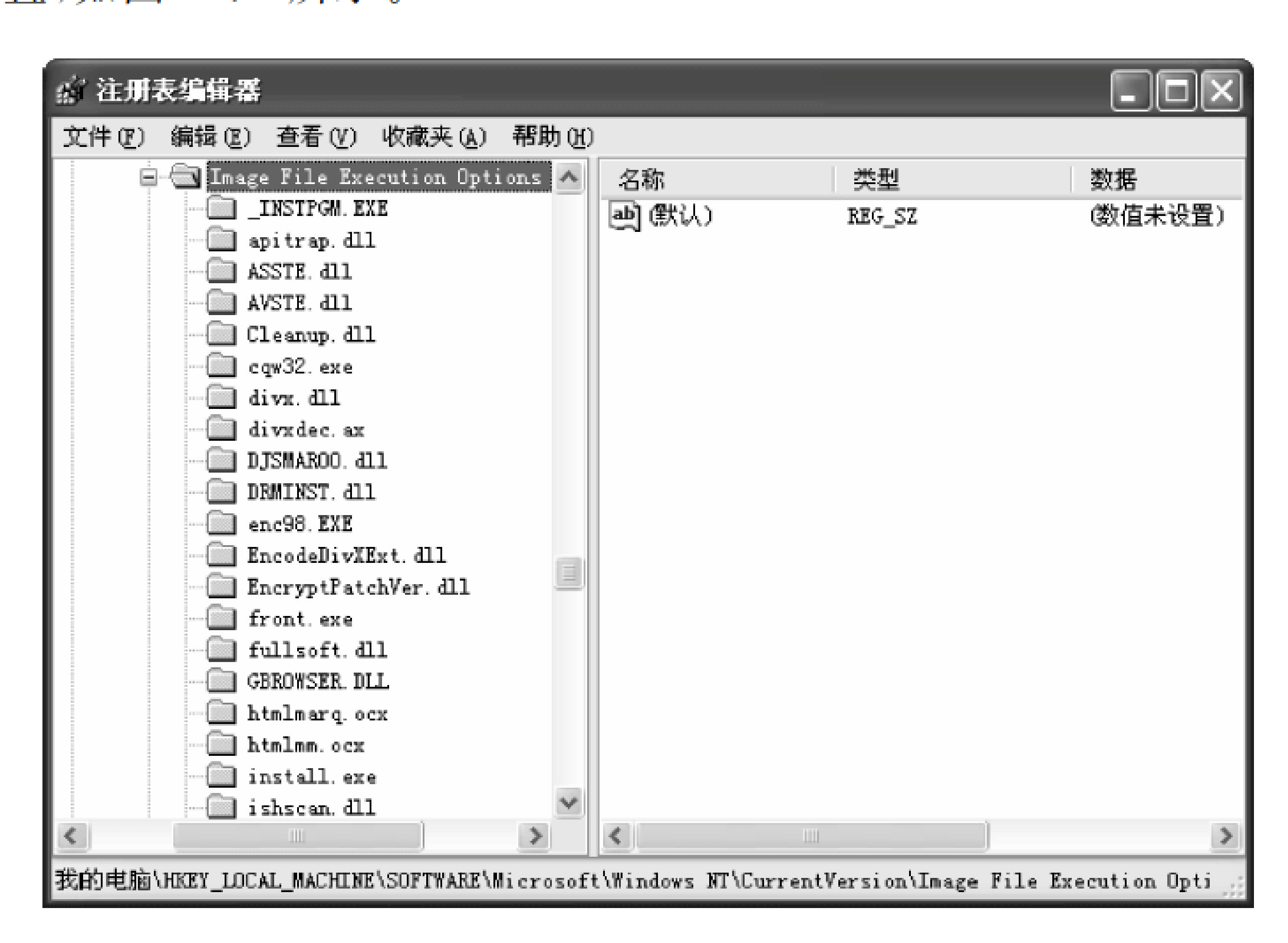


图 17.1 注册表中 IFEO 的位置

在注册表的左栏中,右键单击注册表项 Image File Execution Options,在弹出的快捷菜单中选择"新建"→"项",如图 17.2 所示。然后对新建的注册表子项起一个名字为notepad.exe。

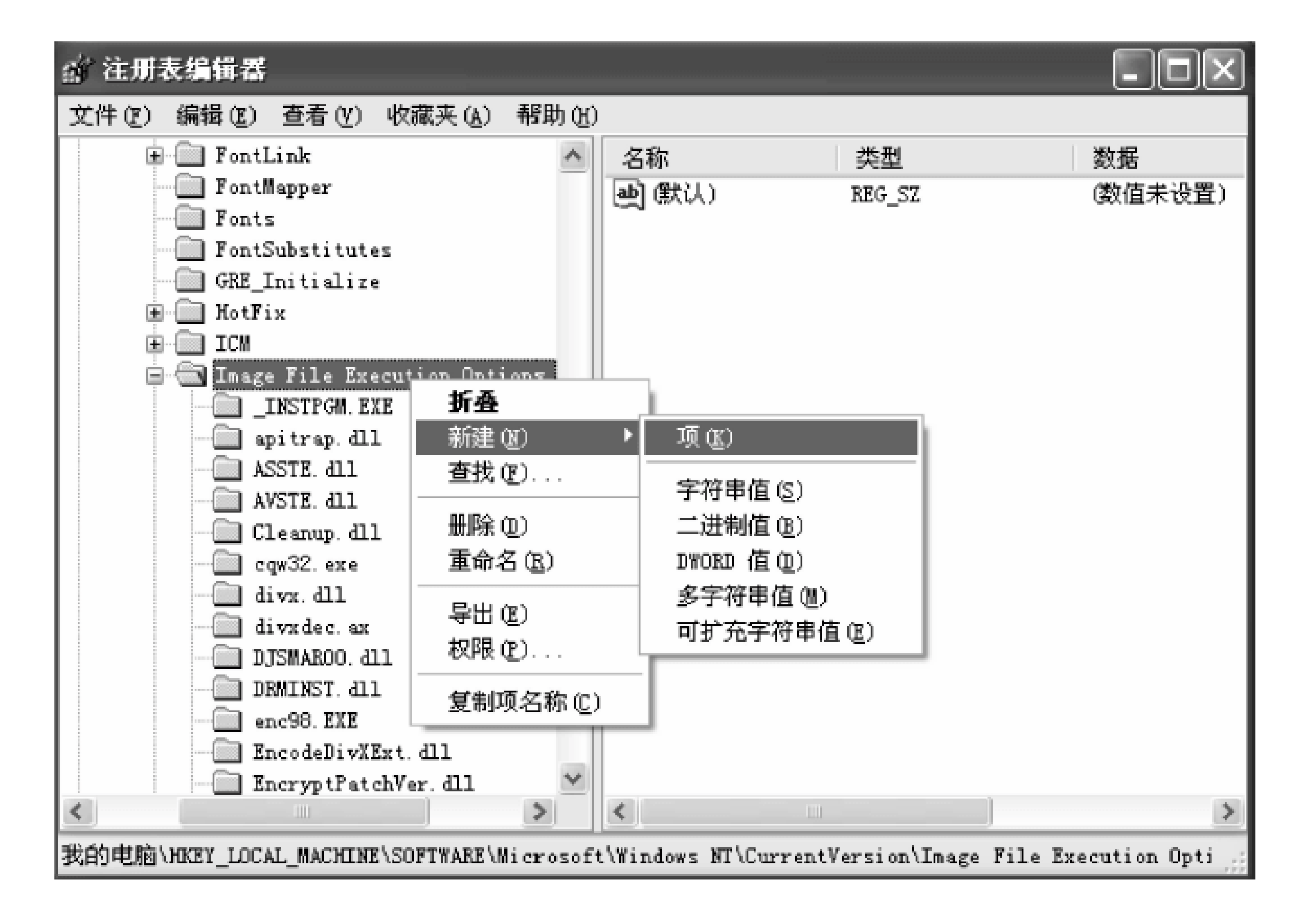


图 17.2 建立新的子项

右键单击新建的子项 notepad.exe,在弹出的快捷菜单中选择"新建"→"字符串值(S)",则会在注册表编辑器右侧新建一个字符串,将其命名为 Debugger,如图 17.3 所示。



图 17.3 创建 Debugger 字符串

双击新建的 Debugger 字符串,在弹出的"编辑字符串"对话框中输入 cmd.exe 的绝对路径,如图 17.4 所示。

关闭注册表,然后在系统桌面上新建一个文本文档,打开该文本文档时,会发现弹出的却是 cmd.exe 的命令行窗口。

同样的道理，病毒和木马也是利用修改注册表的方法，将常见的系统命令甚至安全工具进行映像劫持，使得用户在运行系统命令和安全工具时，打开的却是病毒和木马程序。

图 17.4 设置 Debugger 参数

17.5.2 控制注册表的访问权

由于映像劫持攻击必须通过修改注册表来实现，这样人们可以通过控制注册表访问权的方法来抵制映像劫持工具。

在注册表编辑器中，首先找到 IFEO 的位置，然后在注册表的左侧右键单击 Image File Execution Options，在弹出的快捷菜单中选择"权限"，如图 17.5 所示，从而打开 IFEO 的权限对话框，如图 17.7 所示。

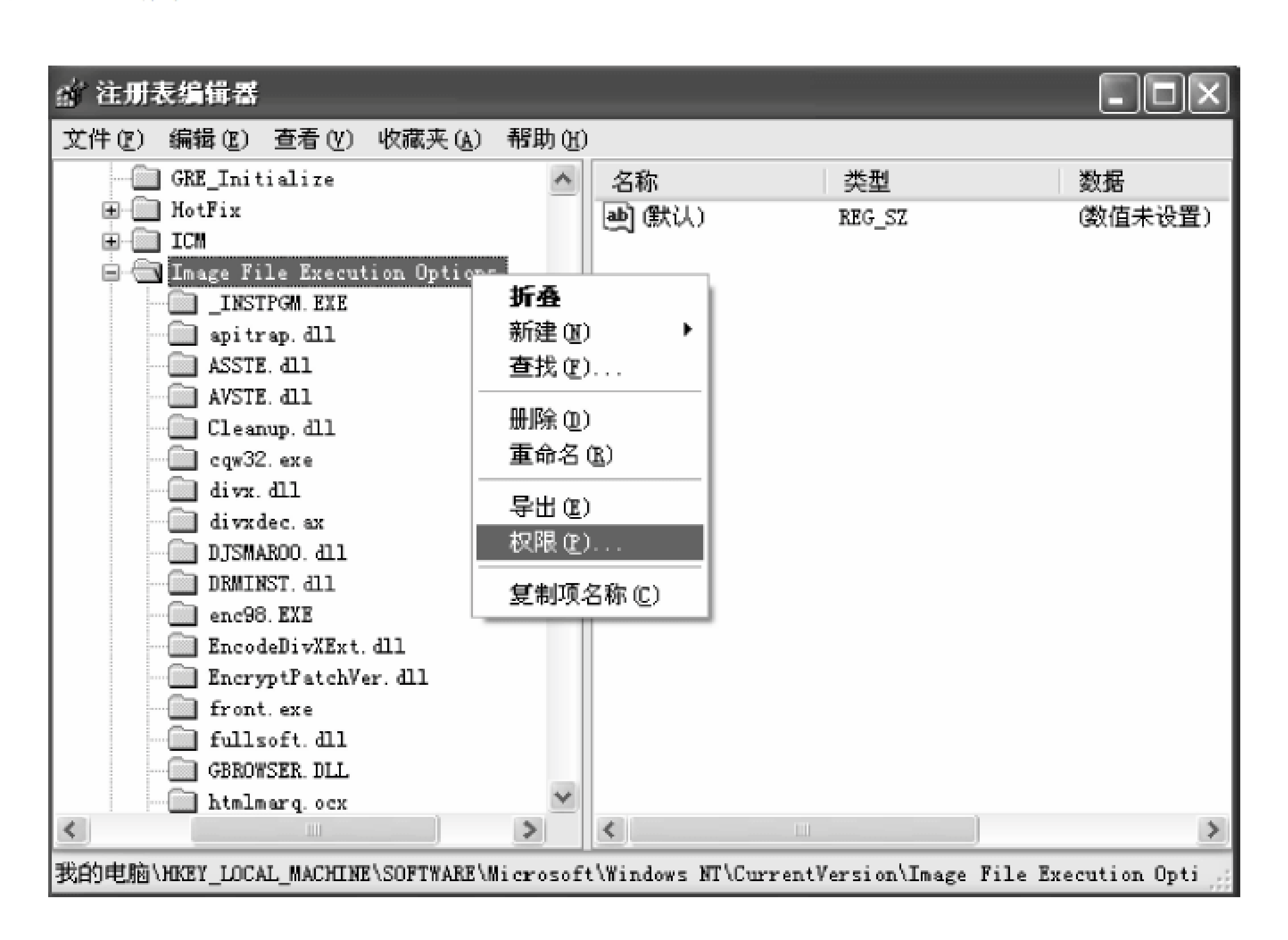


图 17.5 设置 IFEO 的访问权

取消 Administrator 和 system 的创建子项和设置数值的权限。对于 Administrator 可选中图 17.6 中的 Administrator 用户，单击对话框右下角的"高级"按钮，弹出"IFEO 高级安全设置"对话框，如图 17.7 所示。

在图 17.7 中单击 Administrator 用户，然后单击对话框下方的"编辑"按钮，弹出 IFEO 的权限项目对话框，如图 17.8 所示。

在图 17.8 的对话框中，在"允许"列的下方，将"完全控制"、"设置数值"和"创建子项"复选框中的钩取消，然后单击"确定"按钮即完成 Administrator 的权限设置。



图 17.6 IFEO 权限对话框





图 17.7　高级权限设置对话框

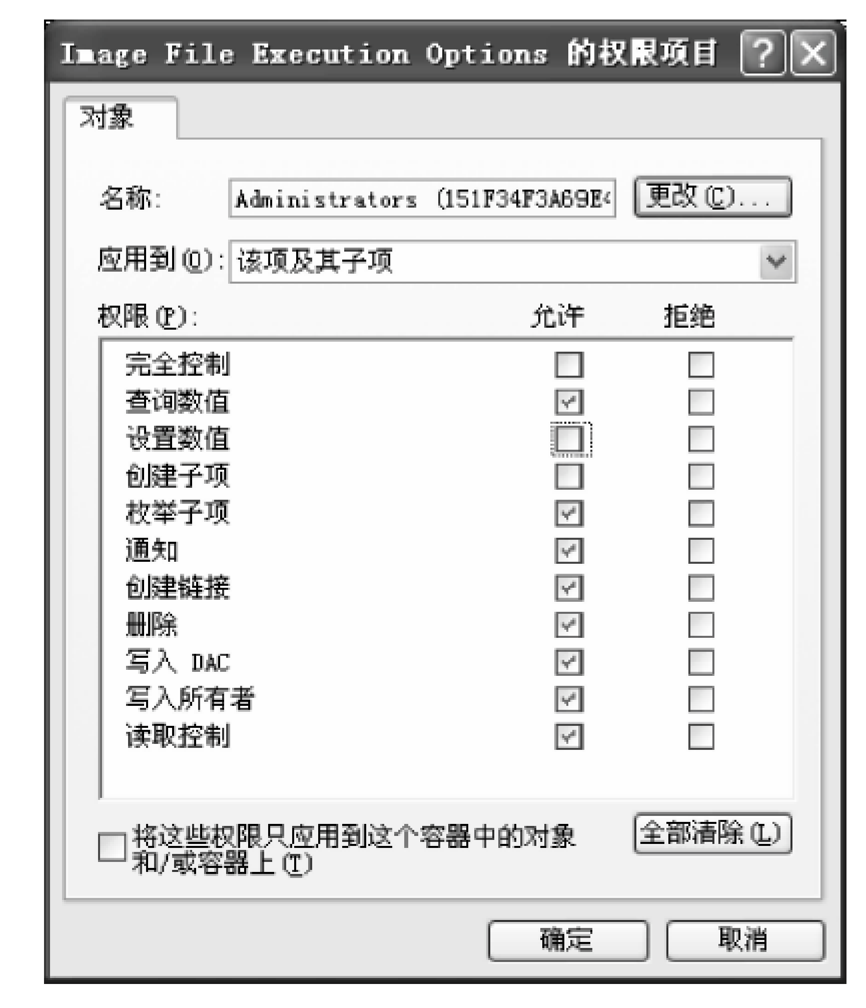


图 17.8　权限项目对话框

17.6　实验思考

（1）在注册表中完成取消 system 账户创建子项和设置数值权限的操作。

（2）通过命令 regedt32. exe 打开注册表编辑器，并验证能否进行注册表权限的设置操作。

实验18 SQL 注入漏洞提权实验

18.1 实验目的与要求

理解基于 SQL 的注入漏洞的原理。

18.2 实验环境

- 两台装有 Windows XP 系统的计算机。
- 一台计算机作为服务器,并安装存在注入漏洞的嘉枫图文管理系统。
- 明小子注入工具 Domain4.1。

18.3 预备知识

SQL(Structure Query Language,结构化查询语句)是一种用于关系型数据库的操作语句,可用于对关系型数据库中的数据表进行插入、删除、更新和查询操作。而 SQL 注入攻击(SQL injection)则是由于 Web 网站的开发人员没有对用户提交的查询语句进行合法性的判断,从而造成 Web 网站向后台网站提供了非法的查询语句,而返回的错误信息中却包含了 Web 数据库的保密信息,如管理员的用户名和密码,最终导致了 Web 网站被非法入侵。

SQL 注入攻击是一种黑客常用的 Web 网站后台数据库攻击手段。这种攻击是从正常的 WWW 端口发起,而且表面来看与一般的 Web 页面访问无区别,因此可以穿过一般的防火墙实施攻击,而不会被发现。除非管理员经常查看日志,否则攻击可以隐藏很长时间。

18.4 实验内容

本章的实验内容主要演示了如何通过明小子注入工具来扫描具有 SQL 注入漏洞的 Web 站点,并如何对这类站点发起注入攻击。

18.5 实验步骤

首先打开明小子注入工具 Domainin 4.1，选择“旁注检测”选项卡，在“当前路径”中输入 Web 服务器的域名或者 IP 地址，如图 18.1 所示。

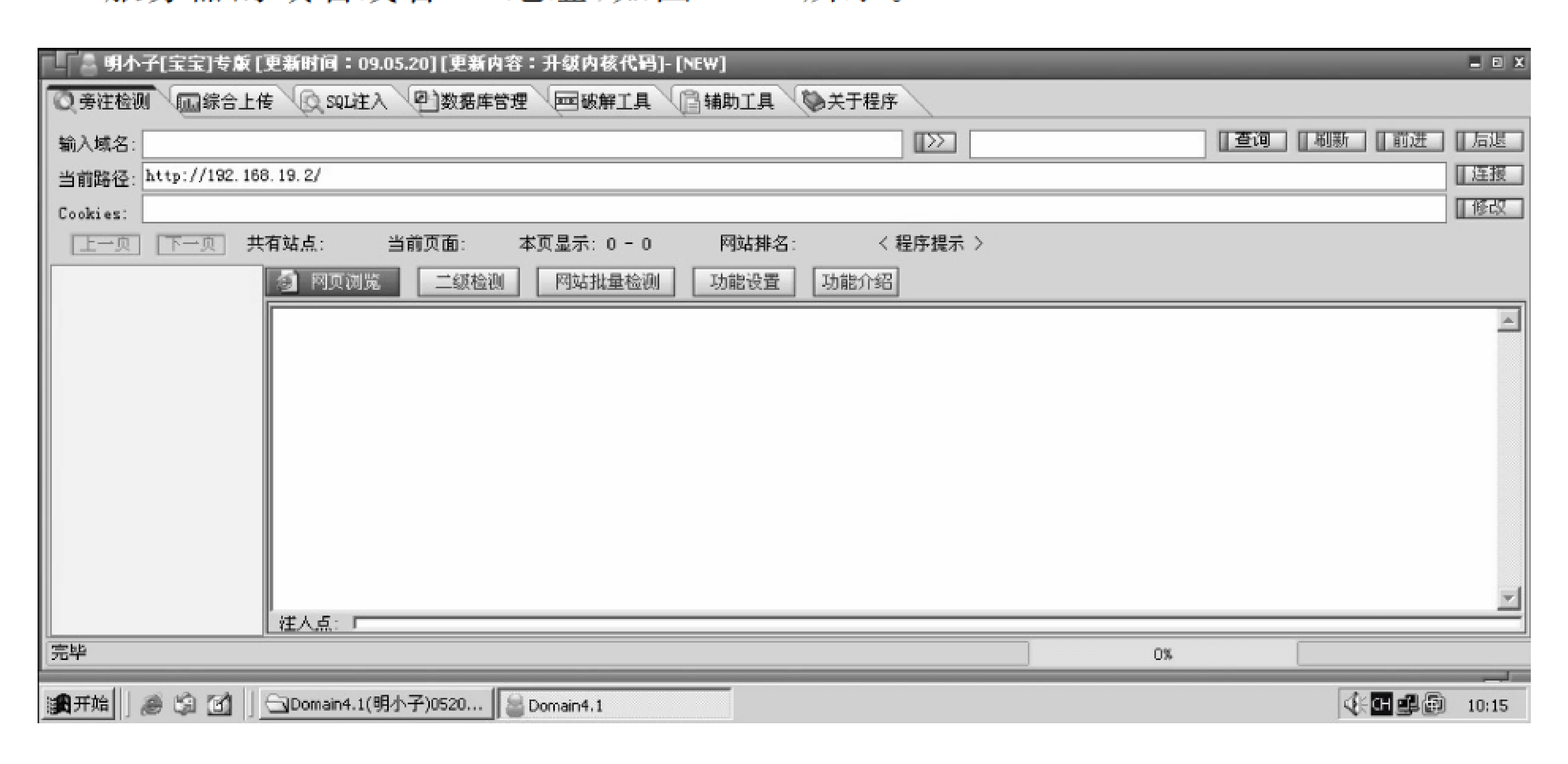


图 18.1　开启 Domain 4.1

单击图 18.1 左上方的“连接”按钮，在“网页浏览”中则会打开相关的网页并自动检测是否存在 SQL 的注入点，并将检测的结果显示采用红色字体显示出来，如图 18.2 所示。



图 18.2　发现注入点

右击图 18.2 下方的任一个注入点，在弹出的快捷对话框中选择"检测注入"命令(如图 18.3所示)，则进入了"SQL 注入猜测检测"阶段，如图 18.4 所示。在如图 18.4 所示的对话框中单击右侧的"开始检测"按钮，经过一段时间后，则会在图 18.5 左下方的"数据库"一栏显示出所检测到的数据表名称。



图 18.3 选择一个注入点



图 18.4 开始注入检测



图 18.5 检测到的数据库名称

选择 admin 数据表，然后单击图 18.5 下方的“猜解列名”，则会显示出 admin 数据表中的字段名称，如图 18.6 所示。



图 18.6 admin 数据表中字段的猜测

选择图 18.6 中“列名”下方的 admin 和 password，单击右侧的“猜解内容”按钮，则会显示出 admin 字段和 password 字段的值，如图 18.7 所示。



排序	admin	password
1	admin	7a57a5a743894a0e

图 18.7 猜测的用户名和密码

从中可以看出管理员的用户名为 admin，而密码为一个 MD5 转换过的值(该值可以通过 Internet 上的在线破译来获取原始的密码值)。

拿到管理员的用户名和密码后，在“管理入口扫描”中进行后台扫描，如图 18.8 所示。

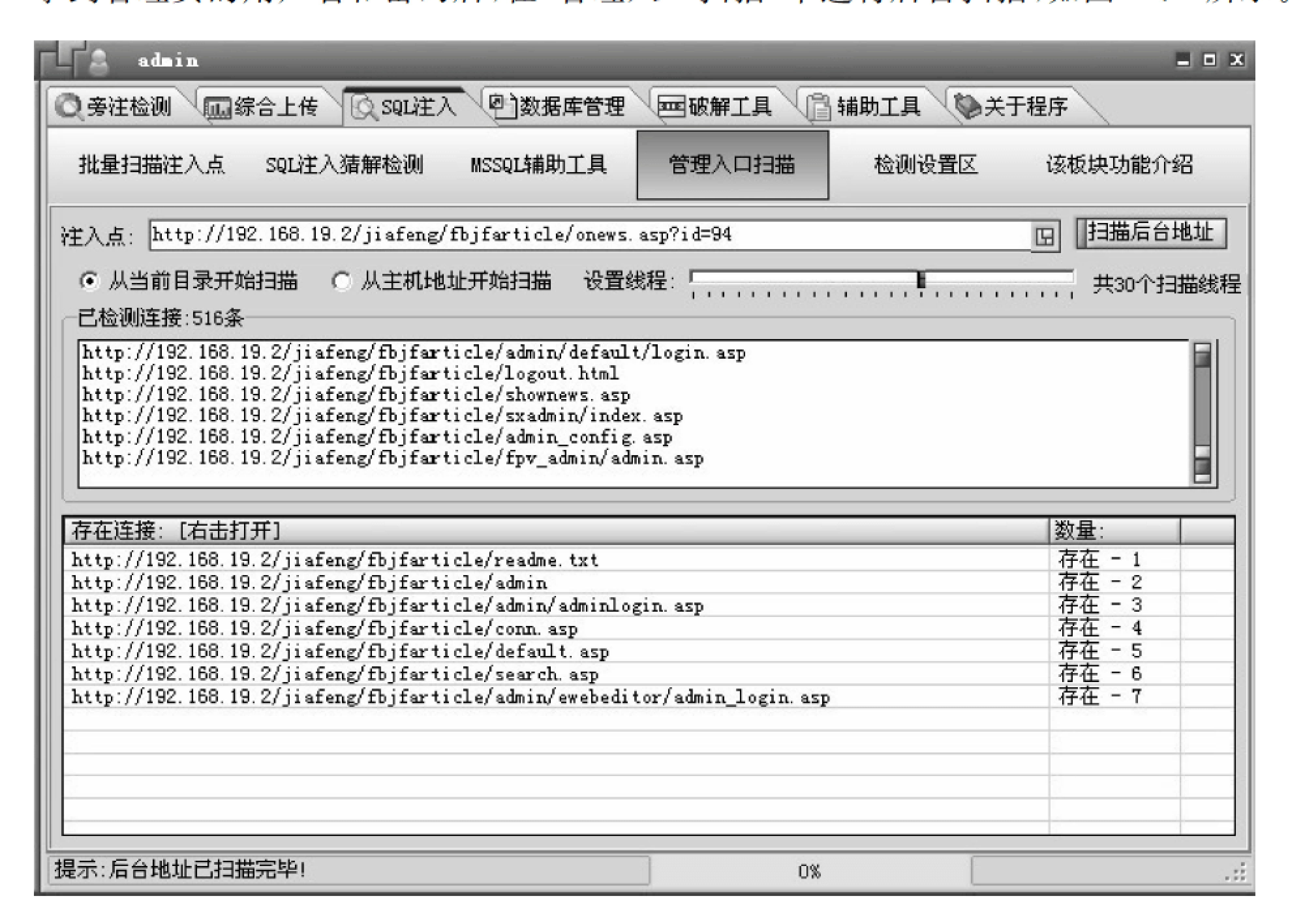


图 18.8 扫描管理入口地址

右击得到的管理入口地址，进入后台登录界面，如图 18.9 所示。



图 18.9 系统后台登录界面

输入刚刚得到的用户名和密码，即可进入后台管理界面，如图 18.10 所示。

图 18.10　后台管理界面

18.6　实验思考

（1）请查阅相关资料，理解出现 SQL 注入漏洞的根本原因。

（2）请查阅相关资料，找到防范 SQL 注入攻击的方法。

参 考 文 献

[1] 冯登国,赵险峰.信息安全技术概论.北京：电子工业出版社,2009
[2] 黄志洪.现代计算机信息安全技术.北京：冶金工业出版社,2004
[3] 张新有.网络工程技术与实验教程.北京：清华大学出版社,2005
[4] 刘嘉勇.信息安全技术实验教程.成都：四川大学出版社,2007
[5] 张玉清,陈深龙,杨彬.网络攻击与防御技术实验教程.北京：清华大学出版社,2010
[6] 田华,李剑,张少芳.网络及信息安全综合实验教程.北京：北京邮电大学出版社,2009
[7] 李剑,信息安全培训教程——实验篇.北京：北京邮电大学出版社,2008

相关课程教材推荐

ISBN	书　　名	定价(元)
9787302183013	IT 行业英语	32.00
9787302239659	计算机专业英语(学术能力培养)	35.00
9787302130161	大学计算机网络公共基础教程	27.50
9787302215837	计算机网络	29.00
9787302235989	数据结构(C 语言版)第 3 版　(另配套实训教材)	25.00
9787302243236	数据结构——Java 语言描述	33.00
9787302246138	计算机组成与汇编语言	29.00
9787302218555	Linux 应用与开发典型实例精讲	35.00
9787302225836	软件测试方法和技术(第二版)	39.50
9787302249177	实用软件测试教程	29.50
9787302221487	软件工程初级教程	29.00
9787302194064	ARM 嵌入式系统结构与编程	35.00
9787302202530	嵌入式系统程序设计	32.00
9787302219668	路由交换技术	29.50
9787302249559	Web 程序设计:ASP.NET	29.50
9787302227151	Web 应用程序设计实用教程	32.00
9787302237556	Java 程序设计实践教程	36.00
9787302244653	C++ 面向对象程序设计	35.00
9787302247487	C# 语言程序设计	23.00
9787302241171	J2EE 应用开发实例精解(WAS+RAD)	25.00
9787302228196	数据仓库与数据挖掘原理及应用	32.00
9787302245384	多媒体技术与应用	32.00
9787302241720	商务智能(第 2 版)	29.50
9787302238195	电子政务概论	36.00
9787302213567	管理信息系统	36.00

以上教材样书可以免费赠送给授课教师,如果需要,请发电子邮件与我们联系。

教学资源支持

尊敬的老师:

感谢您一直以来对清华版计算机教材的支持和爱护。为了配合本课程的教学需要,本教材配有配套的电子教案(素材),有需求的教师可以与我们联系,我们将向使用本教材进行教学的教师免费赠送电子教案(素材),希望有助于教学活动的开展。

相关信息请拨打电话 010-62776969 或发送电子邮件至 liangying@tup.tsinghua.edu.cn 咨询,也可以到清华大学出版社主页(http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn)上查询和下载。

如果您在使用本教材的过程中遇到了什么问题,或者有相关教材出版计划,也请您发邮件或来信告诉我们,以便我们更好地为您服务。

地址:北京市海淀区双清路学研大厦 A-707　　计算机与信息分社 梁颖　收
邮编:100084　　电子邮件:liangying@tup.tsinghua.edu.cn
电话:010-62770175-4505　　邮购电话:010-62786544